ASSOLOMBARDA

2

Quaderni del territorio

# Sicurezza informatica e pirateria software in azienda

## Gestire il rischio e prevenire il problema

2

Quaderni del territorio

# Sicurezza informatica e pirateria software in azienda

## Gestire il rischio e prevenire il problema

La realizzazione di questo quaderno è stata coordinata per Assolombarda da Eugenio Guagnini ed Elena Milanesi.

Il testo è stato curato e redatto da Riccardo Perlusz, Direttore Sicurezza di IBM Italia, con il contributo di Gabriele Fava, Studio Legale Fava e Associati.

Per il supporto alla redazione del capitolo 4, un ringraziamento particolare va a Marco Ornago, già Direttore Divisione Software Originale di Microsoft e Segretario Generale per l'Italia della Business Software Alliance, e allo Studio Legale LGV.

Per i suggerimenti forniti durante la stesura del lavoro, si ringraziano infine i membri del Gruppo di Lavoro sulla Security Aziendale di Assolombarda: Stefania Bertoglio (Alstom Power Italia), Alvise Biffi (Secure Network), Roberto Corno (Linkra), Alberto Della Torre (Carlo Gavazzi Space), Paolo Maria Montalbetti (S.I.P.A. Bindi), Antonio Navassa (EDI Revisione), Ermanno Preo Jr. (Preo), Giorgio Spadoni (Omtra), Lanfranco Zucconi (Carlo Gavazzi Space).

Assolombarda, ottobre 2010

Assolombarda, ottobre 2010

# INDICE

# PREFAZIONE

Questa pubblicazione segna la seconda tappa di un progetto sulla security aziendale avviato da Assolombarda nel 2009 con il Quaderno "Difendere l'impresa. Metodi e strumenti per la prevenzione e la gestione del rischio criminalità".

Con quel primo Quaderno, l'Associazione aveva voluto fornire ad imprenditori e manager un quadro di riferimento introduttivo alla questione; l'obiettivo era quello di sensibilizzare sulla rilevanza del rischio criminalità per la funzionalità e la competitività dell'azienda e diffondere un approccio manageriale alla security aziendale, intesa come ambito di innovazione organizzativa e gestionale.

Con questo secondo Quaderno, il lavoro del 2009 viene ripreso e sviluppato "in profondità" con riferimento ad un aspetto specifico della security aziendale - quello della prevenzione dei reati informatici e, in particolare, del reato della pirateria software - che presenta risvolti tecnici, giuridici e organizzativi complessi e peculiari.

L'obiettivo principale è quello di illustrare la natura del fenomeno e fornire uno strumento che possa essere di immediata utilità pratica per le imprese interessate ad attrezzarsi per proteggersi da questo tipo di reati.

Rispetto al primo Quaderno, che era focalizzato sulla protezione dell'azienda dagli attacchi criminali esterni, questa seconda pubblicazione, inoltre, mette al centro le problematiche di insicurezza e illegalità che, attraverso l'uso degli strumenti informatici, possono essere generate (colposamente o dolosamente) dall'interno dell'azienda.

A questo proposito non si tratta solo di avvertire le imprese di un pericolo, ma di sollecitarle ad assumere un ruolo attivo nel contrasto di un illecito molto diffuso ma poco percepito come tale, attraverso la pianificazione e l'attuazione di misure di prevenzione e controllo che riguarderanno anzitutto l'organizzazione interna dell'azienda.

In questo senso, il Quaderno si colloca nel quadro più generale dell'impegno di Assolombarda per l'affermazione della legalità come componente costitutiva della cultura d'impresa e vuole rappresentare un contributo alla lotta contro l'industria della pirateria software.

**Antonio Colombo**
*Direttore Generale Assolombarda*

# INTRODUZIONE:
## Perché parlare di reati informatici “in” azienda?

Le infrastrutture telematiche e informatiche rappresentano per le aziende uno strumento potente e irrinunciabile per incrementare l’efficienza dei processi di relazione e di comunicazione fra i soggetti coinvolti nelle attività produttive e commerciali. Nel contempo, il loro utilizzo comporta una crescente esposizione a rischi non sempre adeguatamente valutati da imprenditori e manager.

Mentre sono relativamente conosciuti i rischi dovuti alle minacce telematiche generate dai soggetti esterni all’impresa, che attraverso programmi e false comunicazioni cercano di danneggiare i sistemi informatici o di acquisire informazioni utili per successive truffe o frodi, sono spesso sottovalutati i rischi legati ai comportamenti degli agenti interni all’organizzazione (dipendenti, consulenti, fornitori) che, per mezzo di un uso inappropriato delle reti e dei computer aziendali, possono esporre l’impresa a responsabilità dirette e generare danni verso terzi.

Alla luce delle norme sulla pirateria digitale e sulla violazione del diritto d’autore, infatti, di fronte a molti di questi comportamenti l’impresa assume un profilo di responsabilità ed è chiamata ad attuare opportune misure di vigilanza e di riduzione del rischio.

In altri termini: anche se la responsabilità di questi comportamenti è di singoli individui, quando si tratta di collaboratori, dipendenti o fornitori e di fatti avvenuti all’interno dell’azienda, l’impresa stessa e i suoi amministratori finiscono per essere coinvolti in un insieme di responsabilità civili, penali e amministrative e in un danno d’immagine.

I dati oggettivi, rilevati dalle fonti più autorevoli che seguono queste tematiche, indicano che non si tratta più di un problema episodico e che, in particolare per alcuni reati, l’ambito di questi illeciti è sempre il luogo o le attività dell’impresa.

Le dotazioni informatiche individuali di tipo “mobile” usate sia in ambienti controllati (reti aziendali), sia in ambiti meno presidiati e sicuri (abitazioni, altre aziende), la diffusione fra utenze professionali e non dei medesimi prodotti software, la capacità di connessione delle reti telematiche, lo sviluppo di una criminalità professionale nell’ambito del digitale devono far considerare con particolare attenzione queste tematiche.

Occorre essere ben consapevoli che non è più possibile, per chi amministra o dirige un'impresa, sottovalutare o - peggio - ignorare questo insieme di rischi.

Questa pubblicazione affronta il principale e più rilevante rischio per un'impresa che utilizza prodotti ed infrastrutture informatiche: l'uso in azienda di programmi software senza licenza, fatto che determina un illecito penale denominato pirateria software o software piracy.

Nel nostro paese questo reato ha un tasso di diffusione particolarmente elevato, che raggiunge il 48% del prodotto software usato contro una media europea del 33% e del 21% per il Nord America[1].

Alcune recenti leggi hanno definitivamente messo in chiaro che l'uso di programmi software senza licenza è illegale e hanno sancito responsabilità sia individuali sia dei soggetti giuridici coinvolti, quando questi reati avvengono in azienda.

In ragione del suo stretto rapporto con la pirateria informatica, la pubblicazione affronta inoltre anche il tema della violazione del diritto d'autore per i prodotti multimediali, quale reato attuabile nell'impresa anche tramite le infrastrutture telematiche dell'azienda stessa e su cui il titolare o gli amministratori devono porre attenzione.

Va detto che la presenza in azienda di opportune norme e istruzioni che disciplinano efficacemente le condotte dei collaboratori, un'opportuna formazione ed informazione del personale e degli amministratori, un valido sistema di controllo interno riducono non poco, se non annullano, il rischio per l'impresa di incappare in questi reati.

L'obiettivo di questa pubblicazione è quindi duplice. Da una parte, quello di dare all'impresa gli strumenti utili ad identificare e comprendere correttamente questi illeciti e le responsabilità civili, penali ed amministrative che essi generano. Dall'altra, fermo restando che il lavoro non ha per oggetto la normativa lavoristica (con ciò intendendo le problematiche legate all'eventuale applicazione dell'art. 4 dello Statuto dei Lavoratori – L. 300/70), l'obiettivo è quello di fornire concreti suggerimenti e linee guida per la formulazione di norme disciplinari, modalità di intervento e misure organizzative adeguate a gestire il problema.

Nel primo capitolo verrà fornita una introduzione generale al fenomeno della pirateria software con l'obiettivo di chiarire quali sono i casi in cui, uti-

1 Dati rilevati da "Global Piracy Study" 2010, IDC BSA - Maggio 2010

lizzando il software, un'azienda rischia di trovarsi di fronte a questo reato.

Nel secondo capitolo verrà invece affrontata la pirateria software in quanto vera e propria industria criminale e saranno forniti dati sulla sua crescente rilevanza economica a livello mondiale.

Nel terzo capitolo affronteremo gli aspetti giuridici del problema in modo da avvicinarli il più possibile alla realtà imprenditoriale e aziendale, descrivendoli cioè in modo tale che non risultino comprensibili solo a chi fa informatica o si occupa di giurisprudenza.

Il quarto capitolo illustrerà una serie di casi reali in cui sono state coinvolte imprese e che vogliamo condividere per mantenere su un piano di concretezza e realtà il contenuto informativo di questo volume. Non passerà inosservato al lettore come cause (l'uso e l'ingresso in azienda del prodotto illecito) ed effetti (accertamento e giudizio sia civile che penale) della pirateria trovino un ambito comune nelle aziende e come in verità sia possibile e attuabile il contrasto, a cui lavorano più di un soggetto.

Infine, nel quinto capitolo non mancheremo di fornirvi ogni suggerimento utile a determinare le opportune azioni di contenimento del rischio e mitigazione del danno e mostreremo esempi di istruzioni e norme aziendali da attuarsi alla luce dei regolamenti di legge, in contrasto al rischio identificato.

## 1. COSA SONO L'USO ILLECITO DEL SOFTWARE E LA PIRATERIA DIGITALE

L'illecito, meglio noto come **pirateria del software o software piracy**, consiste nell'uso di prodotti software ovvero programmi, applicazioni, sistemi operativi o più semplicemente componenti di un codice sorgente che sono coperti da **diritto d'autore**[2] **o copyright** la cui licenza d'uso non sia stata regolarmente sottoscritta/ottenuta e per la quale quindi non siano stati regolarmente pagati i diritti d'uso dovuti al legittimo titolare del diritto.

Scegliendo da uno scaffale di un rivenditore un pacchetto software tra quelli sopra descritti e pagandolo regolarmente, quasi mai pensiamo che in verità *non lo acquistiamo*, ma otteniamo dal legittimo proprietario la sola **licenza di uso** e più specificatamente la concessione contrattuale di effettuare un determinato numero di installazioni.

La pirateria del software, che fa parte della così detta "pirateria intellettuale", è comunemente intesa come la **duplicazione** o la **distribuzione non autorizzata**, oppure la **copia via download** da un server di rete Internet, la condivisione in ambienti di tipo peer-to-peer, l'**installazione** di diverse copie del **medesimo software**.

Per semplificazione, la pirateria del software avviene quando si può riscontrare uno dei seguenti comportamenti.

**1** L'uso di copie illegalmente prodotte, acquisite all'esterno dell'impresa tramite canali di distribuzione non ufficiali (**software piracy**). Si verifica questo caso quando il personale dell'impresa acquisisce programmi (es. Adobe Acrobat, Office suites, Lotus Notes) o sistemi operativi (es. Microsoft Windows) su siti Internet di file sharing, oppure tramite acquisto o compenso a terzi (in genere venditori abusivi o distributori compiacenti che ne curano la distribuzione illegale) oppure tramite acquisto da siti di commercio elettronico.

Nella software piracy, il software viene installato per uso professionale sui dispositivi informatici di proprietà dell'azienda ed è usato per l'esecuzione delle ordinarie attività.

È importante sottolineare che lo **scopo di profitto** implicato dall'utilizzo in azienda del prodotto illegale genera effetti significativi in termine di responsabilità penale ai sensi di legge, come vedremo più in dettaglio in seguito.

**2** Il diritto consiste di due elementi fondamentali: il diritto morale e il diritto di utilizzazione economica. Il primo è strettamente legato alla persona dell'autore e, salvo casi particolari, tale rimane; il secondo è originariamente dell'autore, il quale può cederlo dietro compenso (ma anche gratuitamente) a un acquirente (licenziatario), il quale a sua volta può nuovamente cederlo nei limiti del contratto di cessione e della legge applicabile, fermi restando i diritti morali.
Il diritto d'autore riconosce al creatore di un'opera una serie di facoltà esclusive per impedire a terzi di sfruttare economicamente la propria opera.
La legge riconosce in particolare la facoltà di pubblicazione, riproduzione, trascrizione, esecuzione, rappresentazione, comunicazione, diffusione, traduzione e/o elaborazione, vendita, noleggio e prestito.

**2** L'uso di una copia originale con licenza per singolo utente/macchina, ma che viene contestualmente installata su più computer (software underlicensed) oppure usata da più utenti client collegati alla medesima applicazione server. È il caso di un prodotto legalmente acquistato dall'impresa, che ne ha quindi acquisito regolare licenza d'uso, ma che (per dolo o colpa) viene poi installato e/o utilizzato su successivi e ulteriori dispositivi informatici. L'illecito può essere compiuto per:

- inadempienza del personale a disposizioni operative di merito, che diligentemente l'impresa ha predisposto ed impartito;
- negligenza dei responsabili dell'azienda nel gestire e far gestire correttamente le risorse informatiche;
- negligenza o malafede di fornitori incaricati della gestione e manutenzione delle piattaforme informatiche, come ad esempio nei contratti di *Fleet Management o di Maintenance&Repair*;[3]
- precisa volontà dell'impresa o dei suoi incaricati di agire illecitamente.

Ciascuna di queste possibile condizioni, nel corso di eventuali verifiche ispettive da parte delle autorità preposte, comporterà sanzioni amministrative e/o denunce penali in base alle risultanze degli accertamenti.

**3** L'uso del software in ambiente difforme da quello contrattualmente previsto (software mislicensed). È il caso delle licenze subordinate a particolari condizioni d'uso, che una volta acquisite vengono destinate ad usi e condizioni diverse rispetto a quanto contrattualmente sottoscritto (es. prodotti di disegno industriale CAD ad uso software accademico, programmi installati con la clausola del Try&Buy, programmi con licenza gratuita freeware o shareware ma solo per installazione o uso non produttivo o lavorativo).

**4** La cessione a terzi e la rivendita del software (software mis-reselled) laddove questa è espressamente negata nelle clausole di licenza del prodotto. È il caso ad esempio di dismissione o rivendita delle piattaforme informatiche aziendali per rinnovo tecnologico o per altre iniziative.

**3** Ambedue le forme di servizio offerte all'impresa da parte di provider IT costituiscono modalità con cui vengono gestite le piattaforme di informatica individuale.
Il fornitore si occupa della fornitura, riparazione e sostituzione del personal computer del dipendente assegnatario per conto dell'impresa.

Come per le altre opere dell'ingegno anche la produzione di software e dei codici informatici che lo costituiscono è tutelata dal diritto d'autore.

Diversamente dal tradizionale ambito di tutela, per i programmi software la titolarità dell'opera appartiene ad un soggetto diverso da quello che ha materialmente realizzato il prodotto.

Il diritto d'autore, la cui tutela giuridica è stata introdotta nel nostro ordinamento giuridico a partire dal 1941 per tutelare le opere tradizionali d'ingegno quali la musica, lo spettacolo, la letteratura, ha dovuto tener conto dell'uso sempre più esteso delle nuove tecnologie di produzione, di comunicazione e di tutti i nuovi ambiti della multimedialità digitale, completando negli ultimi anni un'evoluzione legislativa tanto complessa quanto irrimandabile.

Considerato che il prodotto digitale è alla base del funzionamento di qualsiasi elettronica programmabile oggi disponibile (da un telefono cellulare ad un megacentralino telefonico, da un piccolo computer palmare sino a un robusto server industriale, dal modem wifi di casa sino al router di rete che distribuisce miliardi di informazioni al secondo) l'oggetto di riferimento per la legislazione ha raggiunto un valore economico complessivo e una potenzialità di creare danni economici e sociali incalcolabili.

Gli effetti negativi della violazione del diritto d'autore si riflettono su interessi privati e pubblici. La duplicazione e la distribuzione illegale di queste opere, infatti, arrecano un danno economico a:

- i titolari dei diritti di sfruttamento delle opere, con l'evasione del diritto d'autore;
- l'erario, con l'evasione delle imposte dirette e indirette;
- le aziende produttrici, che hanno investito nella progettazione e realizzazione, per la mancata vendita del prodotto e conseguente perdita di fatturato;
- il mercato, per la creazione dei presupposti della concorrenza sleale fra le imprese che usano prodotti leciti (a costo) e le imprese che usano prodotti non leciti (a costo ridotto o nullo);
- l'utente finale, per il potenziale danno generabile dall'uso di un prodotto con qualità tecniche scadenti o inaffidabile.

Quest'ultimo punto è particolarmente rilevante. Chi usa consapevolmente o non questi prodotti per attività produttive è esposto a dei rischi importanti. È infatti emerso da alcuni studi tecnici condotti su copie di software

pirata, che un'alta percentuale di questi prodotti ha del "codice applicativo" aggiuntivo non raramente costituito da *malware* capace di causare danni ai sistemi informatici che lo ospitano o programmato per rivelare dati a terzi.

Queste modifiche, che rendono il prodotto utilizzabile anche senza codice di licenza, comportano una ridotta funzionalità rispetto al prodotto originale e non consentono l'installazione delle eventuali modifiche tecniche emesse dal produttore per la correzione di problemi e per il mantenimento operativo del prodotto. Il software piratato è un prodotto che in breve tempo è destinato a divenire instabile o incompatibile con gli altri prodotti dell'ambiente IT in cui è installato.

La pirateria non è solo un danno economico, ma anche una sfida per la crescita delle imprese. Da quando l'uso illecito dei prodotti software, la clonazione abusiva dei prodotti e/o l'illecita acquisizione delle chiavi di accesso ai programmi (password) sono entrati nell'impresa, vi sono ulteriori motivi per condividere e supportare azioni dirette ad un contrasto più efficace di questi illeciti da parte dell'azienda stessa.

Se è infatti evidente l'esigenza di preservare i legittimi diritti di chi ha investito per lo sviluppo e per la commercializzazione dei prodotti, è altrettanto importante sottolineare la necessità di mantenere la corretta concorrenzialità fra le imprese che li utilizzano. Vi è infatti una chiara differenza tra l'utilizzo di un determinato prodotto regolarmente licenziato (il cui costo peserà su i costi d'impresa e quindi sul prezzo di ciò che verrà poi offerto al cliente) e l'utilizzo illecito dello stesso programma a costi più bassi o comunque inferiori.

La pirateria, infine, è anche un danno al sistema paese, perché alimenta l'illegalità diffusa e costituisce il business di vere e proprie organizzazioni criminali. A differenza di altre realtà del mercato dell'illecito digitale, quali ad esempio la musica o i programmi destinati ai videogiochi, la pirateria del software dipende infatti principalmente da una produzione e distribuzione organizzata del prodotto illecito.

Affiancato da una pirateria individuale, svolta da singoli soggetti non professionisti, nei luoghi di lavoro o nel proprio domicilio, il mondo dell'illecito organizzato è un'area in continua espansione.

## 2. UN FENOMENO IN ESPANSIONE

### 2.1 La fabbrica dell'illecito: perché aumenta l'offerta di prodotto

Quantificare il fenomeno della contraffazione, data la sua natura, è impossibile se non attraverso valutazioni induttive, che derivano dai volumi di prodotti sequestrati nel corso di attività di polizia tributaria e giudiziaria.

Il danno generato dalla pirateria digitale nel 2007 in Italia ammonta a 2,6 miliardi di euro ed è calcolato considerando il solo materiale distribuito attraverso un supporto fisico. Il valore del danno sarebbe nettamente superiore se si potesse sommare anche lo scambio online tramite P2P che però, per la sua caratteristica, sfugge ad ogni rilevazione e costituisce di fatto un canale ben superiore a quello del supporto fisico.

Nel 2007 il materiale sequestrato ha visto il sorpasso dei file multimediali relativi ai filmati video (334,6 milioni di euro) rispetto a quelli musicali (261,4 milioni di euro), ma i contenuti più piratati continuano ad essere il software applicativo e i programmi per videogiochi.

Sempre nel 2007, le perdite causate dalla duplicazione illegale dei programmi software hanno raggiunto 1.150 milioni di euro contro i 907 del 2006, valore che per il solo segmento professionale si avvicina ad un tasso di illegalità stimato intorno al 49% nelle piccole e medie imprese.

Diverse e successive ricerche hanno portato a formulare interessanti valutazioni in merito all'evoluzione della pirateria software, che si configura oramai come vero e proprio business criminale organizzato su scala internazionale.

I mercati con economie emergenti in forte crescita e, contestualmente, con sistemi giuridici deboli (es. Cina, India, Asia, Est Europa, Sud America), dove il grado di tutela della proprietà intellettuale e i relativi mezzi di contrasto sono evidentemente ridotti, sono le aree in cui si stanno generando fenomeni impressionanti in termini di domanda di software illecito.

Questa domanda stimola le attività di ricerca e acquisizione di prodotti illeciti da parte di soggetti criminali che, grazie alle debolezze organizzative e distributive dei produttori di software e alle potenzialità telematiche offerte dalla rete internet, operano a livello transnazionale per poter fornire un'offerta di prodotto.

Di contro, l'opportunità di prodotti da cui generare copie illegali è disseminata nei paesi più prossimi alla maturità di investimento IT, dove è naturalmente presente una grande quantità e scelta di prodotto clonabile oltre a tutte le tecnologie utili a perpetrare l'illecito e dove sono presenti infrastrutture di rete Internet di ampia capacità e basso prezzo (P2P, high band) utilizzabili per la distribuzione.

La pirateria software, con la duplicazione illegale e la contraffazione del prodotto e dei suoi marchi, è un'attività illegale che la casistica giudiziaria ascrive a:

- duplicatori professionali, che producono e distribuiscono con tecniche industriali;
- duplicatori non occasionali, che agiscono attraverso la rete Internet e con mezzi tecnici specifici;
- singoli soggetti, quali comuni utilizzatori, che spesso agiscono senza saper neppure di commettere un illecito e senza una finalità diretta di profitto.

I prodotti "tipici" della pirateria software sono:

1 Copie di programmi software derivanti dalla riproduzione illegale di un prodotto tramite duplicazione dei suoi supporti di memorizzazione. Eseguite a partire dal prodotto originale "sprotetto" da organizzazioni criminali per mezzo di impianti tecnici adeguati, sono realizzate in modo da renderle riconoscibili e riconducibili al prodotto originale, senza tuttavia cercare di costruirlo in modo identico. La distribuzione è realizzata tramite una rete distributiva presente sul territorio che sfrutta rivenditori compiacenti.

2 Copie contraffatte di un prodotto commerciale originale. Sono eseguite a partire dal package (imballo, documentazione) e dai marchi distintivi originali che vengono contraffatti e usati per confezionare il prodotto illecito. Anche in questo caso la produzione è realizzata da organizzazioni criminali che operano con attrezzature e tecnologie semi-industriali.

3 Copie di molteplici programmi su un unico supporto di memorizzazione. Sono realizzate da duplicatori non occasionali che acquisiscono prodotti contraffatti e "sprotetti" attraverso molteplici fonti della rete Internet, per poi commercializzarli su un unico supporto fisico.

**4** Copie di prodotto software pre-installato su personal computer.
Sono realizzate quando il venditore di un prodotto hardware, in fase di personalizzazione dell'offerta di vendita o per rendere maggiormente interessante la proposta di acquisto, installa prodotti contraffatti e privi di licenza d'uso sul dispositivo.

Oggi i tassi di pirateria in Europa Occidentale rappresentano il 36% del software installato, con una perdita stimata di circa 9.600 milioni di dollari. Nei paesi occidentali, con economie in controtendenza, la contraffazione è sempre meno legata all'utente non professionale ed è sempre più presente nelle aziende.

In particolare, i fattori che favoriscono la crescita del fenomeno nel nostro paese, in controtendenza rispetto al resto dei paesi EU, sono la sempre maggior presenza di piccole e medie imprese e di utenti professionali privati, soggetti che si rivelano spesso:

- inconsapevoli del problema;
- con poche risorse da dedicare alla corretta gestione delle attività;
- disposti a sostenere il rischio approfittando della maggior disponibilità di software illecito, che grazie alla rete Internet e alle applicazioni P2P è facilmente rintracciabile e scaricabile da qualsiasi area del mondo tramite connessioni telematiche.

## 2.2 Incremento della domanda: il problema dentro l'impresa

Con l'evoluzione dei nuovi modelli informatici, sempre più spesso viene a cadere la separazione fra il software destinato all'utente *professionale* e quello destinato all'utente *consumer* e i prodotti offerti dal mercato sono spesso i medesimi, con soluzioni disegnate e distribuite contestualmente sulle diverse piattaforme operative disponibili, comprese quelle tipiche delle infrastrutture telematiche usate nelle imprese stesse (linux, windows, unix).

Allargando la base dei prodotti installabili, si ampliano contestualmente la domanda di prodotti illeciti e le fonti e gli strumenti utili per la loro acquisizione.

Al fenomeno della standardizzazione del prodotto e dei mercati "uniformati" si è aggiunto l'uso sempre maggiore dei dispositivi portatili, che vengono adoperati sia in ambienti controllati dall'impresa, sia in situazioni più "permeabili" o meno sicure.

Dove non esiste opportuna informazione o controllo, non è raro che le condotte individuali siano meno attente a evitare i rischi generati da un'offerta così penetrante.

È noto, per altro, che il reato o l'illecito informatico viene compiuto più facilmente perché non percepito come tale. Se per usare un prodotto informatico non originale dovessimo appropriarcene indebitamente dallo scaffale di un negozio o sottrarlo dall'abitazione di qualcuno, probabilmente ci renderemmo immediatamente conto della illiceità dell'azione.

Altra importante considerazione è in merito alla facilità con cui può accadere che il materiale illecito entri in azienda. A questo proposito si possono identificare diverse casistiche significative:

- materiale acquisito direttamente dai dipendenti, tramite relazioni dirette di tipo personale con conoscenti, congiunti, colleghi;
- materiale trasferito ai dipendenti da fornitori abituali che hanno relazioni continuative o da visitatori temporanei (es. stagisti), che per motivi diversi hanno temporaneamente operato con l'informatica dell'impresa;
- materiale acquisito inconsapevolmente attraverso normali forniture commerciali oppure a causa di particolari operazioni (es. acquisizione societarie);
- materiale scaricato via rete Internet dal personale, tramite relazione diretta con soggetti terzi (forum, chatting, siti web) o scaricato attraverso siti per il download con protocolli P2P.

La rete Internet non solo amplifica le possibilità di ricerca a livello transnazionale, ma di fatto rende più "neutra" la percezione del reato commesso e del contatto con strutture o persone con le quali ordinariamente la maggior parte di noi non vorrebbe avere a che fare.

La falsa percezione di anonimato e di sicurezza che la relazione telematica può generare spesso porta a far sì che lo stesso *utilizzatore-acquisitore* diventi a sua volta un *distributore-venditore di illecito*, con le conseguenze che queste azioni possono avere da un punto di vista della responsabilità penale.

Non è affatto raro che questi illeciti avvengano nei luoghi di lavoro, attraverso le infrastrutture dell'impresa, all'insaputa dei titolari o dei responsabili stessi, su cui tuttavia ricadranno potenzialmente alcune responsabilità di legge.

In ultimo, una condizione economica di difficoltà come quella attualmente vissuta dalle imprese può portare erroneamente a pensare di poter tagliare i costi attraverso soluzioni (l'illecito) considerate come *temporanee,* ma che spesso diventano un *definitivo* compromesso.

# 3. INQUADRAMENTO GIURIDICO

## 3.1 Le nuove norme di tutela del diritto d'autore per i programmi informatici.

La tutela giuridica del software, come oggi è attuata, è il risultato di un complesso percorso legislativo iniziato a partire dagli anni '90 quando il diritto d'autore, così come originariamente interpretato dalla L. 633/1941, è stato esteso all'informatica, alle nuove tecnologie della comunicazione e alle opere d'ingegno che i nuovi media telematici utilizzano.

Art. 171 bis - Legge sul diritto d'autore (L. 633/1941) e successive modifiche

1. Chiunque abusivamente duplica, per trarne profitto, programmi per elaboratore o ai medesimi fini importa, distribuisce, vende, detiene a scopo commerciale o imprenditoriale o concede in locazione programmi contenuti in supporti non contrassegnati dalla Società italiana degli autori ed editori (SIAE), è soggetto alla pena della reclusione da sei mesi a tre anni e della multa da lire cinque milioni a lire trenta milioni.

   La stessa pena si applica se il fatto concerne qualsiasi mezzo inteso unicamente a consentire o facilitare la rimozione arbitraria o l'elusione funzionale di dispositivi applicati a protezione di un programma per elaboratori. La pena non è inferiore nel minimo a due anni di reclusione e la multa a lire trenta milioni se il fatto è di rilevante gravità.

2. Chiunque, al fine di trarne profitto, su supporti non contrassegnati SIAE riproduce, trasferisce su altro supporto, distribuisce, comunica, presenta o dimostra in pubblico il contenuto di una banca di dati in violazione delle disposizioni di cui agli articoli 64 quinquies e 64 sexies, ovvero esegue l'estrazione o il reimpiego della banca di dati in violazione delle disposizioni di cui agli articoli 102 bis e 102 ter, ovvero distribuisce, vende o concede in locazione una banca di dati, è soggetto alla pena della reclusione da sei mesi a tre anni e della multa da lire cinque milioni a lire trenta milioni. La pena non è inferiore nel minimo a due anni di reclusione e la multa a lire trenta milioni se il fatto è di rilevante gravità.

Prima di questa sostanziale modifica della norma e nel pieno della diffusione delle tecnologie telematiche, un palese vuoto legislativo aveva contribuito a generare una sorta di "zona franca" dei comportamenti individuali e collettivi. Per anni il dibattito fra brevettabilità e diritto d'autore, quale mezzo per la tutela giuridica del software, aveva di fatto bloccato lo sviluppo di ogni possibile norma a garanzia dei produttori e degli investitori che, a seguito di questa situazione, avevano interpretato il segmento dei prodotti programma per elaboratori come un'area di rischio per gli investimenti, invece che come un potenziale mercato attrattivo.

Tuttavia, quasi a voler recuperare il tempo allora perso, dal novanta a oggi la normativa ha subito una continua accelerazione nella sua evoluzione legislativa.

Con il D.Lgs. 518/1992, la legislazione italiana ha recepito la Direttiva 1991/250/CEE in materia di tutela giuridica del software[4] e - inserendo l'articolo 171 bis nella Legge sul diritto d'autore – ha introdotto anche nel nostro Paese la tutela del software.

È il primo di una serie di atti legislativi che modificheranno nella sostanza l'originario diritto d'autore per adeguarlo al radicale sviluppo tecnologico che, in più di mezzo secolo dalla prima legge di riferimento, ci ha trascinato a distanza di ere rispetto a quel contesto.

Negli anni successivi al 1992, a fronte delle diverse interpretazioni dei legislatori, l'art. 171 bis subirà alcune progressive modificazioni[5], rimanendo tuttavia il punto di riferimento giuridico ineludibile per il contrasto della pirateria software e quindi anche per la prevenzione all'interno dell'azienda dei rischi ad essa connessi.

Con questo insieme di interventi legislativi, la legge sul diritto d'autore applicato ai programmi software ha esteso elementi di garanzia e di diritto nel segmento di mercato dei prodotti programma per elaboratori e nelle banche dati informatiche. In particolare il nuovo assetto legislativo, rispetto al periodo precedente, ha stabilito alcune importanti novità.

Prima fra tutte e forse la più innovativa, la possibilità da parte del titolare dei diritti o di un suo legale rappresentante di attuare incisive azioni civili che consentono un'azione di verifica a fronte di possibili illeciti, azioni condotte tramite Ufficiali Giudiziari e consulenti tecnici nominati da tribunale civile.

È stata poi introdotta la sanzione penale[6] per le violazioni che vengano ritenute ai sensi di legge rilevanti e sono state inasprite le pene, che prevedendo importanti sanzioni ausiliarie quali la sanzione pecuniaria, il sequestro, l'inibitoria, la pubblicazione della sentenza.

Dalla nuova struttura legislativa emerge un concetto cardine: il contesto in cui il reato è consumato è fondamentale per determinarne le responsabilità, che si estendono nell'impresa oltre al solo soggetto individuale.

Chi infatti detiene o utilizza all'interno della propria attività imprenditoriale o professionale programmi software di natura illecita, ovvero in assenza di

**4** Con percorsi paralleli, attraverso la L. 547/1993 il nostro ordinamento disciplina comportamenti che costituiscono illeciti prodotti con l'uso della nuove tecnologie e istituisce i delitti chiamati appunto reati informatici, caratterizzati dalla previsione che l'attività illecita abbia come oggetto o mezzo del reato un sistema informatico o telematico. Alcuni di questi reati vengono associati alla violazione del diritto, perché costituiscono il mezzo con cui gli illeciti sulla proprietà intellettuale sono di fatto realizzati. Le nuove fattispecie di reato sono:

- esercizio arbitrario delle proprie ragioni (art. 392 C.P.)
- attentato ad impianti di pubblica utilità (art. 420 C.P.)
- falsità in documenti informatici (art. 491 bis C.P.)
- accesso abusivo ad un sistema informatico (art. 615 ter C.P.)
- detenzione e diffusione abusiva di codici di accesso (art. 615-quater C.P.)
- diffusione di programmi diretti a danneggiare o interrompere un sistema informatico (art. 615-quinquies C.P.)
- violazione della corrispondenza e delle comunicazioni informatiche e telematiche (art. 616, 617-quater, 617-quinquies, 617 sexies C.P.)
- rivelazione del contenuto di documenti segreti (art. 621 C.P.)
- trasmissione a distanza di dati (art. 623 bis C.P.)
- danneggiamento di sistemi informatici o telematici (art. 635 bis C.P.)
- frode informatica (art. 640 ter C.P.).

Nell'ambito della presente pubblicazione alcuni dei reati suddetti verranno successivamente meglio trattati per ricondurli all'obiettivo di questo lavoro.

**5** Tali modificazioni sono state apportate con la L. 248/2000, con il D.Lgs. 68/2003, con il D.L. 72/2004, convertito in L. 128/2004 e con il D.L. 7/2005, convertito con modificazioni dalla L. 43/2005.

**6** È prevista la reclusione da 6 mesi a 3 anni e una multa da euro 2.582,28 fino a euro 15.493,71.

evidenza fiscale e amministrativa del regolare acquisto o della detenzione, compie un reato che comporta conseguenze per il soggetto individuale responsabile delle violazioni di legge (che può essere per altro individuato anche negli amministratori e dirigenti dell'impresa), ma anche per il soggetto giuridico stesso (l'impresa), che in base alle nuove norme di legge è ritenuto responsabile anche di porre in atto prescritte misure di controllo e di verifica del rischio.

In base alle ultime modifiche dell'art. 171 bis, l'elemento soggettivo del reato si configura già solo in presenza di una finalità di profitto e non più, come nelle prime formulazioni di legge, con il fine di lucro.

Ciò rende di fatto applicabile la sanzione penale in tutti i casi in cui la violazione è direttamente riconducibile a una attività d'impresa, escludendo ogni possibilità di interpretazione dell'illecito quale violazione contrattuale compiuta ai danni del titolare dei diritti.

Proseguendo nella valutazione dell'evoluzione legislativa, rileviamo anche che il D.Lgs. 68/2003 recepisce definitivamente le indicazioni della Direttiva 2001/29/CEE sull'armonizzazione della disciplina del diritto d'autore, introducendo ulteriori novità sui sistemi anticopia e, conseguentemente, nuove sanzioni per chi riproduce un'opera violando tali sistemi di protezione.

Con la L. 128/2004, meglio conosciuta come Legge Urbani, sono state inoltre apportate nuove modifiche alla normativa in tema di file sharing e di pirateria online e sono state disposte sia sanzioni amministrative per coloro che scaricano dalla rete contenuti protetti da diritto d'autore, sia sanzioni penali per gli utenti che condividono con altri soggetti e attraverso Internet le opere protette dal diritto d'autore.

Infine, nel 2009, con le modifiche apportate dal cosiddetto Decreto Sicurezza al D.Lgs. 231/2001, i delitti in violazione del diritto d'autore entrano pienamente nel novero della ormai nota normativa sulla responsabilità amministrativa dell'impresa, aprendo nuovi scenari circa l'onere che oggi ricade sull'impresa nell'attuare al proprio interno una disciplina particolare nell'ambito dell'uso degli strumenti informatici.

Le nuove norme di legge costituiscono non solo un punto di svolta per il contrasto alla pirateria informatica, ma anche un sostanziale cambiamento per le politiche di sicurezza delle aziende, che sono chiamate ad attuare:

- un maggior **controllo per autotutela** e per non vedersi chiamate a rispondere di fatti delittuosi generati al proprio interno;
- precisi **piani di riduzione del rischio** al fine di acquisire l'esonero dalle eventuali responsabilità amministrative così come previsto dalle recenti norme (D.Lgs. 231/2001).

Oggi, infatti, in caso di accertamento della presenza in azienda di software illegale o di strumenti applicativi atti a rimuovere le misure di protezione dei programmi, possono essere **ritenuti responsabili** anche i **titolari o gli organi di gestione e controllo della società** stessa. In particolare, l'Amministratore Delegato e i membri del consiglio di Amministrazione per le società di capitali ovvero i soci nel caso delle società di persone.

Per altro le nuove norme hanno reso più veloci le **procedure d'accertamento**, che oggi possono essere espletate:

- tramite la **Forza di Polizia** deputata alle ispezioni ed accertamenti (Polizia Economica – Guardia di Finanza), con la possibilità di eseguire controlli autonomi a sorpresa, senza dover preventivamente informare la controparte o agire in attuazione di specifiche indagini giudiziarie;
- da parte di un **Ufficiale Giudiziario** in esecuzione di un apposito decreto emesso da un magistrato (sede civile) ed attuato da un **Consulente Tecnico d'ufficio** nominato dal Tribunale, che avrà quindi pieno titolo per effettuare una ricognizione tecnica sui dispositivi informatici presenti in impresa.

Quest'ultimo caso assicura di fatto il pieno diritto delle aziende produttrici dei programmi software e dei singoli titolari del diritto d'autore di agire già in sede civile nei confronti di presunte violazioni, per consentire in una forma semplificata e più celere la reale verifica e l'acquisizione di eventuali prove per la successiva azione legale.

Cosa suggeriamo di fare

- ☑ Verificate periodicamente attraverso l'inventario dei prodotti software aziendali la copertura delle licenze per tutti gli utilizzatori effettivi
- ☑ Nel caso di difformità, provvedete nell'immediato a sanare la situazione
- ☑ Non autorizzate l'installazione "autogestita" di prodotti software già presenti in azienda
- ☑ Non trasferite all'utilizzatore aziendale il materiale originale del prodotto (CD, DVD, UserId o n. licenza originale)

Se a seguito dell'esecuzione della ricognizione è accertata la presenza di prodotti software non licenziati, il titolare dei diritti può richiedere ed ottenere un risarcimento calcolato in base al valore commerciale e al numero di copie illegali rinvenute, nonché la liquidazione di un danno morale.

Spesso nelle verifiche in azienda di un illecito relativo alla violazione dell'art. 171 bis, gli accertamenti evidenziano ulteriori reati computi con finalità sussidiarie, che possono aggravare la situazione dell'impresa e dei suoi amministratori.

La tabella 1 riporta i principali reati sussidiari associabili alla violazione del diritto d'autore e consente rapidamente di comprendere la potenziale esposizione al rischio generata da una violazione all'interno dell'azienda; si pensi ad esempio al caso di uno o più dipendenti che duplichino abusivamente del software, lo confezionino riproducendone le etichette e gli imballaggi e lo rivendano via rete telematica.

**Tabella 1** - Principali violazioni penali connesse alla pirateria software

| Fattispecie | Testo di legge | Articolo di legge | Reato consumato | Sanzione associata |
|---|---|---|---|---|
| Violazione del diritto d'autore | L. 633/1941 | Art. 171 bis comma 1 | Duplicazione abusiva di programmi a scopo di profitto | Reclusione da sei mesi a tre anni e multa da euro 2.582 a euro 15.493 |
| | L. 633/1941 | Art. 171 bis comma 2 | Importazione, distribuzione, detenzione, vendita o noleggio di copie di programmi a scopo commerciale o imprenditoriale | Reclusione da sei mesi a tre anni e multa da euro 2.582 a euro 15.493 |
| | L. 633/1941 | Art. 171 bis | Rimozione arbitraria o elusione funzionale di dispositivi applicati a protezione del programma | Reclusione da sei mesi a tre anni e multa da euro 2.582 euro 15.493 |
| Contraffazione marchi | Codice Penale | Art. 473 | Contraffazione o uso illecito di marchi o segni distintivi di opere d'ingegno o di prodotti industriali | Reclusione da tre a dodici anni e con la multa da lire un milione a sei milioni |
| Frode commerciale | Codice Penale | Art. 474 | Introduzione in commercio di prodotti o di opere d'ingegno con segni o marchi falsi | Reclusione fino a due anni e con la multa fino a lire quattro milioni |
| | Codice | Art. 517 | Porre in circolazione industriali o opere d'ingegno con segni mendaci o contraffatti | Reclusione fino a un anno o con la multa fino a lire due milioni |

## 3.2 La responsabilità dell'impresa

Diamo ormai per scontato che non sia più possibile escludere che un soggetto all'interno dell'impresa duplichi e distribuisca prodotti software all'insaputa dei responsabili dell'azienda, svolgendo quindi quelle attività illecite di cui abbiamo ampiamente trattato nei paragrafi precedenti.

È un fenomeno non voluto, ma indirettamente generato dalla contemporanea presenza di una informatica a basso prezzo, di strumenti ad alta potenzialità tecnologica, di una generalizzata non percezione del reato o dei rischi ad esso collegati e dalla diffusione della pirateria digitale sia come fenomeno criminale organizzato, sia come comportamento individuale.

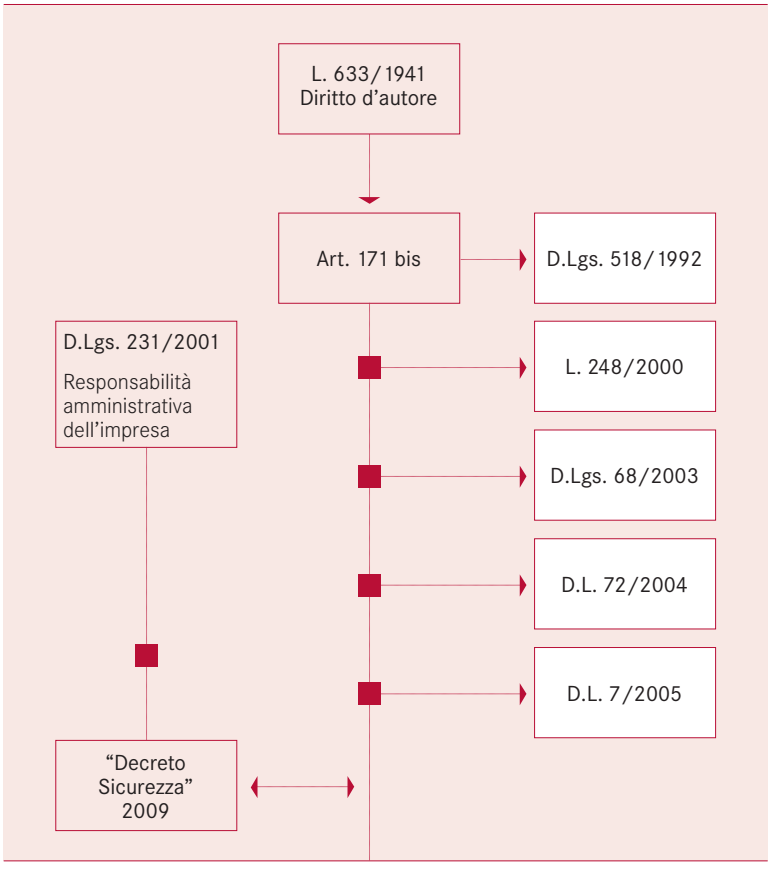


**Figura 1** Evoluzione della legge sulla responsabilità amministrativa dell'impresa e relazione con la legge sul diritto d'autore

Se non vi fosse stata la rete Internet e se non si fosse spostato nell'ambito delle attività professionali e dell'impresa, l'illecito sarebbe rimasto probabilmente confinato nell'ambito dei modelli della contraffazione tradizionale, condotta da pochi e con produzioni di dimensione e modalità industriale.

Questo delitto, invece rientra ormai nella categoria definita dai criminologi come "criminalità massiva" proprio per la sua diffusione fra soggetti non ordinariamente criminali e per la difficoltà di rilevarne l'estensione.

Le infrastrutture telematiche, i supporti fisici e i dispositivi di maggior potenza presenti nelle aziende rispetto a quelli disponibili in altri ambiti non lavorativi, l'adozione dei personal computer portatili e del loro software sono state le cause evidenti per cui questi illeciti sono emersi nei luoghi di lavoro.

Abbiamo visto però che questi comportamenti costituiscono nel nuovo ordinamento legislativo una condotta illecita che rientra nell'ambito dell'azione penale verso l'impresa, quando questi reati avvengono appunto nell'ambito di un'attività commerciale o imprenditoriale[7] o se vengono compiuti con scopo di profitto: il risparmio per il mancato acquisto della licenza può di fatto costituire un profitto e, nell'esercizio delle attività d'impresa, il software detenuto illegittimamente contribuisce in modo sostanziale a un ricavo.

Pur essendo la responsabilità penale sempre soggettiva e imputabile alla sola persona fisica, i rappresentanti dell'impresa rispondono del delitto, quando viene provata la conoscenza diretta o indiretta circa l'utilizzazione abusiva del software[8].

Oltre alla responsabilità penale ascrivibile alla persona fisica e alla responsabilità amministrativa ascrivibile alle persone giuridiche, il nostro ordinamento, con il D.Lgs. 231/2001, ha anche riconosciuto una sorta di responsabilità "penale amministrativa" delle persone giuridiche, introducendo un nuovo regime di "responsabilità" a carico degli enti e derivante dalla commissione, o tentata commissione, di determinate fattispecie di reato, nell'interesse o a vantaggio degli enti stessi.

La responsabilità amministrativa prevista dal decreto consente di colpire (direttamente tramite sanzioni pecuniarie o indirettamente tramite, ad esempio, l'interdizione dall'esercizio dell'attività) il patrimonio degli enti, e quindi l'interesse economico dei soci che hanno tratto un vantaggio dalla

**7** L'attività imprenditoriale di beni e servizi si ha sempre dove l'organizzazione del lavoro, delle risorse e della tecnologia prevalga sull'apporto individuale.

**8** In caso diverso, la responsabilità è dei singoli dipendenti che risulteranno aver uso esclusivo o certo del dispositivo informatico o dei supporti di memorizzazione che contengono il materiale illecito eventualmente rilevato.

commissione di determinati reati da parte delle persone fisiche che rappresentano l'ente o che operano per l'ente.

I reati per i quali l'ente può essere chiamato a rispondere sono soltanto quelli espressamente indicati dal legislatore:

- reati nei rapporti con la Pubblica Amministrazione;
- delitti informatici e trattamento illecito di dati;
- reati di falso nummario;
- reati societari;
- reati con finalità di terrorismo o di eversione dell'ordine democratico ;
- reati contro la personalità individuale;
- reati di abuso di mercato;
- reati di omicidio colposo e lesioni colpose gravi o gravissime, commessi con violazione delle norme antinfortunistiche e sulla tutela dell'igiene e della salute sul lavoro;
- ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita;
- reati transnazionali.

L'ente è responsabile se il reato è stato commesso a "suo interesse o a suo vantaggio" (D.Lgs. 231/2001, art. 5, comma 1); non è pertanto necessario aver conseguito un "vantaggio" concreto, ma è sufficiente che sussista "l'interesse" a commettere il reato.

Il decreto prevede anzitutto che gli enti forniti di personalità giuridica, le società e le associazioni siano passibili di responsabilità amministrativa per reati commessi a loro vantaggio o nel loro interesse da:

- persone che rivestono funzioni di rappresentanza, amministrazione o direzione o da chi esercita anche di fatto funzioni di direzione e controllo;
- persone sottoposte alla direzione o vigilanza di uno dei soggetti indicati al punto precedente.

Ma, per alcuni reati, il decreto prevede anche che - se la condotta illecita è stata realizzata nell'interesse o a vantaggio di un ente - la responsabilità in sede penale degli enti si aggiunge a quelle delle persone fisiche che li rappresentano e che materialmente hanno realizzato l'illecito.

Anche in questo caso però la società non risponde se è provato che le persone hanno agito nell'interesse esclusivo proprio o di terzi.

È importante sottolineare che il decreto prevede l'esonero dalle responsabilità qualora la società dimostri che:

- sono stati adottati, prima della commissione del fatto illecito, modelli di organizzazione, gestione e controllo idonei a prevenire la realizzazione degli illeciti penali considerati;
- sono stati identificati i rischi in relazione ai reati che possono essere commessi e alle attività nel cui ambito possono essere commessi reati;
- sono stati adottati un codice etico e un sistema di sanzioni disciplinari applicabili in caso di mancato rispetto delle misure previste dal modello, al fine di conservarne l'effettività;
- è stata fornita adeguata comunicazione al personale e sua formazione con riferimento particolare al codice etico;
- sono stati previsti specifici protocolli tesi a programmare la formazione e l'attuazione delle decisioni societarie in relazione ai reati da prevenire;
- sono state individuate le modalità di gestione delle risorse finanziarie idonee ad impedire la commissione dei reati;
- è stato affidato a un organo interno dotato di poteri di iniziativa e controllo il compito di vigilare sul funzionamento e sull'osservanza del modello;
- sono stati previsti obblighi di informazione nei confronti dell'organismo incaricato di vigilare sul funzionamento e sull'osservanza dei modelli;
- le persone che hanno commesso l'illecito hanno agito fraudolentemente;
- non è stato omesso il controllo previsto.

Le due fasi principali attraverso le quali si creano i modelli sono quindi quella dell'identificazione dei rischi e quella della progettazione del sistema di controllo. Nella prima fase si deve analizzare il contesto aziendale per individuare le probabilità e le modalità di commissione dei reati; mentre nella seconda fase si progetta il modello, tenendo anche conto degli eventuali strumenti di controllo interni già esistenti. L'organismo di controllo è chiamato a svolgere prevalentemente compiti di vigilanza e verifica dell'adeguatezza del modello, analisi sul mantenimento nel tempo dei requisiti di solidità e funzionalità del modello ed eventuali aggiornamenti che si dovessero rendere necessari.

L'adozione del modello di organizzazione e gestione è prevista dal D.Lgs. 231/2001 in termini facoltativi. Tuttavia, la sua adozione è sicuramente consigliata, dal momento che la presunzione di responsabilità dell'ente per il reato commesso da un soggetto in posizione apicale (art. 5), può es-

sere superata solamente dimostrando la validità e l'efficiente attuazione del modello di organizzazione che è stato predisposto. La sola adozione del modello da parte dell'organo dirigente non rappresenta, tuttavia, misura sufficiente a determinare l'esonero da responsabilità dell'ente, essendo infatti necessario anche che:

- il modello sia gestito con continuità, curandone l'aggiornamento a seguito di modifiche organizzative e normative;
- ne sia periodicamente monitorata l'efficacia;
- ne sia verificata l'osservanza con riferimento alle aree a rischio.

Per operare efficacemente, il sistema brevemente delineato non può ridursi ad un'attività *una tantum*, bensì deve tradursi in un processo continuo (o comunque svolto con una periodicità adeguata), da reiterare con particolare attenzione nei momenti di cambiamento (apertura di nuove sedi, ampliamento di attività, acquisizioni, riorganizzazioni, ecc.).

L'esonero della responsabilità dell'ente passa quindi attraverso il giudizio di idoneità del sistema interno di organizzazione e di controllo.

L'applicazione della cosiddetta "esimente", in occasione di procedimento penale per uno dei reati considerati dal D.Lgs. 231/2001, è subordinata alla positiva valutazione, da parte del giudice penale, dell'idoneità del modello organizzativo e gestionale a prevenire la commissione di tali reati.

Il modello di organizzazione e di gestione è, pertanto, il mezzo attraverso il quale l'ente ha l'opportunità di dimostrare la propria diligenza organizzativa (premiata appunto con l'esimente o la riduzione dell'afflittività delle sanzioni).

L'adozione di un modello organizzativo che renda le procedure interne più trasparenti, oltre a garantire l'esenzione dalla responsabilità amministrativa, costituisce quindi un'occasione di crescita e sviluppo per le imprese, migliorando, da un lato, il loro rapporto con la società e, quindi, la loro immagine pubblica di efficienza, trasparenza ed etica commerciale e, dall'altro, riducendo i costi di transazione derivanti da eventuali azioni legali e da processi di contrattazione.

Come anticipato nel precedente paragrafo, nel luglio del 2009, attraverso il Decreto Sicurezza, è stato aggiornato l'elenco dei reati per cui il D.Lgs. 231/2001 prevede la responsabilità dell'impresa, allargandolo anche ai

delitti in violazione del diritto d'autore, ovvero:

- l'abusiva duplicazione a fini di profitto di programmi per elaboratore;
- l'importazione, la distribuzione, la vendita e detenzione a scopo commerciale o imprenditoriale o la concessione in locazione di programmi contenuti su supporti privi di contrassegno SIAE;
- la predisposizione di mezzi atti a eludere o asportare i dispositivi di protezione di un programma per elaboratore.

Per questi reati, la norma ha previsto una pesante sanzione pecuniaria fino a 500 quote, calcolata appunto tramite il sistema che la legge ha introdotto per la definizione del valore della sanzione.

Per maggior precisione ricordiamo che la nuova normativa prevede sia sanzioni pecuniarie sia sanzioni interdittive.

Le prime, oltre alla riparazione per danni causati dal reato, alla eventuale restituzione di utili percepiti illecitamente, prevede appunto una sanzione pecuniaria calcolata in quote. Più precisamente, un importo unitario di singola quota moltiplicato il numero di quote che il magistrato determinerà essere applicabile ai fini dell'efficacia della sanzione.

L'importo di ogni singola quota va da un minimo di 258 euro sino ad un massimo di 1.549 euro in base alla gravità della condotta, al profilo economico e patrimoniale dell'ente. Il numero delle quote va da un minimo di 100 ad un massimo di 1.000 in base alla gravità della violazione e alla responsabilità dell'ente.

La combinazione valore*numero quote determina una sanzione che va da un minimo di 25.800 euro sino a un massimo di 1.549.000 euro.

Le sanzioni interdittive previste nei casi più gravi e inflitte anche congiuntamente alle pene pecuniarie prevedono confisca del profitto, divieto di pubblicizzare beni e servizi dell'azienda, divieto di contrattare con la Pubblica Amministrazione, sospensione o revoca di autorizzazioni, licenze e finanziamenti.

In sintesi:

- la pirateria software in azienda non è più solo un rischio amministrativo;
- sanzioni penali possono coinvolgere l'impresa ed i suoi amministratori quando non è provata la loro estraneità;
- da luglio 2009 la pirateria del software è entrata nel novero dei reati che generano responsabilità amministrativa per l'impresa.

## 4. IMPARARE DAGLI ERRORI: I CASI AVVENUTI PRESSO LE AZIENDE

Considerare lontano dalle nostre aziende l'ipotesi di un possibile controllo e quindi sottovalutare il problema, non affrontando o rimandando oltre tempi utili un'azione organizzativa, è un errore che va sicuramente evitato.

Lo dimostreranno i casi che sono stati raccolti in questo capitolo grazie al contributo dell'Associazione internazionale BSA – Business Software Alliance. BSA raggruppa i principali produttori di software a livello mondiale e, a favore dei propri associati, svolge un'azione di prevenzione e contrasto della pirateria software.

In ragione delle peculiari capacità tecnico-operative che la caratterizzano, l'Associazione si è però qualificata anche come punto di riferimento per le stesse autorità giudiziarie.

Come evidenzieranno i casi di seguito presentati, la collaborazione tra autorità giudiziarie e soggetti di natura privata come la BSA è un fattore decisivo per la lotta alla contraffazione di marchi e prodotti industriali e più in generale per la diffusione di una cultura della legalità nella gestione del software all'interno del mondo dell'impresa.

Anche se nella restituzione che ne offriremo verrà garantito l'anonimato ai soggetti coinvolti, va sottolineato che i casi raccolti sono tutti relativi a vicende giudiziarie realmente accadute.

## 4.1 Quando l'impresa e le sue regole sono assenti

L'ampia legislazione e l'organizzazione della magistratura in specifiche sezioni presso i Tribunali consentono alle aziende titolari dei diritti d'autore di agire contro la pirateria digitale in modo diretto, efficace e in tempi brevi.

Dato l'elevato livello di interazione operativa e informativa delle imprese con soggetti terzi, l'illecito relativo ai prodotti software utilizzati in azienda è quasi impossibile da occultare o mimetizzare e spesso emerge in modo palese all'insaputa dell'impresa stessa.

È il tema di questo primo caso, in cui l'azione legale del danneggiato, che utilizza le misure messe a disposizione dalla nuova legislazione, consente di far emergere una situazione di palese illegalità.

La società Autodesk, leader mondiale nella fornitura di software di progettazione 2D e 3D per i settori edilizio, industriale, delle infrastrutture, dei mezzi di comunicazione e dello spettacolo, produttrice e titolare dei diritti sul software e associata a BSA, riceve una segnalazione relativa al presunto utilizzo senza alcuna licenza di copie di software di sua titolarità presso la società **α**, società del settore immobiliare di Milano.

I programmi per elaboratori della Autodesk sono oggi particolarmente diffusi, perché costituiscono strumenti tecnici essenziali per la progettazione architettonica e per il disegno tecnico di prodotti industriali per le imprese.

I medesimi prodotti, inoltre, sono ampiamente utilizzati per la lettura di informazioni e dati anche da parte dei successivi attori della filiera, come ad esempio società terziste che provvedono alla produzione fisica dei manufatti o società di servizi che riutilizzano i disegni dei progettisti per ulteriori attività commerciali, come nel caso in esame.

In particolare, sono proprio le aziende di questo tipo, che dovendo necessariamente adottare lo standard imposto dal generatore del dato ed intravvedendo nell'acquisto regolare del software unicamente un costo addizionale, lasciano che vengano usate dai propri dipendenti copie illecite.

Tornando al caso in esame, il fatto che il software privo di licenza non fosse direttamente utilizzato nella attività *core* dell'azienda può aver favorito la sottovalutazione della rilevanza dell'illecito segnalato a BSA.

Di fronte a tale segnalazione, la prima operazione condotta da BSA è la verifica della presenza di registrazioni di licenza per i prodotti segnalati,

verifica che viene condotta attraverso l'analisi dei dati amministrativi e gestionali ordinariamente utilizzati dai propri associati ai fini dell'assistenza al cliente e della garanzia.

Riscontrata grazie a BSA l'assenza di tali registrazioni, nell'ottobre 2009 Autodesk incarica il suo studio legale di fiducia di depositare un ricorso avanti il Tribunale di Milano, Sezione specializzata in materia di proprietà industriale e intellettuale, al fine di richiedere un provvedimento che autorizzi la descrizione, l'accertamento e la perizia ai sensi dell'art. 171 bis della L. 633/1941 e dell'art. 128 del D.Lgs. 30/2005[9] dei programmi per elaboratore di sua titolarità ed utilizzati da α.

Si deve considerare che, soprattutto in materia di software, i precedenti giurisprudenziali sono concordi nel ritenere che il provvedimento di descrizione, accertamento e perizia debba essere concesso *inaudita altera parte*, ossia "a sorpresa".

E infatti, il Tribunale di Milano autorizza la descrizione, accertamento e perizia *inaudita altera parte* dei programmi in questione, da eseguirsi presso la sede di α, nonché presso altre sue sedi secondarie.

Il provvedimento viene eseguito dopo solo 3 settimane, con la presenza dell'ufficiale giudiziario competente, assistito dal perito tecnico nominato dal Tribunale (CTU), oltre che da rappresentanti legali e tecnici di Autodesk.

L'ufficiale giudiziario si reca presso la sede societaria e convoca il legale rappresentante di α, al quale notifica il provvedimento del Tribunale di Milano e comunica le ragioni dell'intervento, intimando che al CTU tecnico sia permesso l'accesso a tutti i computer e supporti informatici presenti nella sede dell'azienda.

Per poter permettere la corretta esecuzione del provvedimento, i dipendenti della società α devono inoltre sospendere la propria attività. L'ufficiale giudiziario intima altresì che tutti i dipendenti si astengano dal modificare in qualsiasi modo la situazione del parco informatico aziendale e in particolare non modifichino o cancellino o in qualsiasi altro modo alterino la situazione dei software di Autodesk.

Successivamente, il perito tecnico dà inizio alle "operazioni di descrizione", ovvero all'analisi dei singoli computer e delle informazioni relative ai programmi software su questi installati, che richiederanno un'in-

**9** D. Lgs. 30/2005 Codice della proprietà industriale, a norma dell'articolo 15 della legge 12 dicembre 2002, n. 273, pubblicato nella Gazzetta Ufficiale n. 52 del 4 marzo 2005 - Supplemento Ordinario n. 28.

Art. 128. Descrizione
1. Il titolare di un diritto industriale può chiedere che sia disposta la descrizione degli oggetti costituenti violazione di tale diritto, nonché dei mezzi adibiti alla produzione dei medesimi e degli elementi di prova concernenti la denunciata violazione e la sua entità.
2. L'istanza si propone con ricorso al Presidente della sezione specializzata del tribunale competente per il giudizio di merito, ai sensi dell'articolo 120.
3. Il Presidente della sezione specializzata fissa con decreto l'udienza di comparizione e stabilisce il termine perentorio per la notificazione del decreto.
4. Lo stesso giudice, sentite le parti e assunte, quando occorre, sommarie informazioni, provvede con ordinanza non impugnabile e, se dispone la descrizione, indica le misure necessarie da adottare per garantire la tutela delle informazioni riservate e autorizza l'eventuale prelevamento di campioni degli oggetti di cui al comma 1. Quando la convocazione della controparte potrebbe pregiudicare l'attuazione del provvedimento, provvede sull'istanza con decreto, motivato, in deroga a quanto previsto al comma 3.
5. L'ordinanza di accoglimento, ove la domanda sia stata proposta prima dell'inizio della causa di merito, deve fissare un termine perentorio non superiore a trenta giorni per l'inizio del giudizio di merito.
6. Il provvedimento perde di efficacia se non è eseguito nel termine di cui all'articolo 675 del codice di procedura civile.
7. Si applica anche alla descrizione il disposto dell'articolo 669-undicies del codice di procedura civile.

tera giornata e che consentiranno di rinvenire ben 53 programmi di titolarità di Autodesk (principalmente programmi Autodesk AutoCAD in varie versioni) tutti installati e funzionanti sui 79 computer presenti presso **α**, per un valore che si aggira intorno ad euro 300.000.

La dimensione dell'illecito rinvenuto e l'ampia e puntuale distribuzione dei prodotti illeciti all'interno della struttura operativa di **α** lasciano pochi dubbi sia sulla capacità che sulla volontà dell'impresa di gestire correttamente le attività informatiche, dotando degli opportuni programmi (ovviamente licenziati) le stazioni di lavoro dei dipendenti.

In assenza di controlli da parte dell'azienda e lasciata la situazione alla gestione individuale dei dipendenti, realizzatasi con un disastroso autoreperimento del prodotto, non vi è da meravigliarsi che l'illecito si sia propagato all'intera rete telematica aziendale.

Quando l'ufficiale giudiziario richiede alla società **α** di esibire le licenze relative ai programmi rinvenuti, questa si trova nell'impossibilità di rispondere adeguatamente.

Le evidenze portano quindi a certificare nei fatti che la società **α** utilizza, senza licenze d'uso, tutti i programmi per elaboratore di titolarità di Autodesk installati sui personal computer oggetto di analisi e descrizione presso i locali utilizzati come sede.

Emerge inoltre che la maggior parte dei programmi erano stati illecitamente scaricati da Internet e si evidenzia come l'assenza di opportune politiche di sicurezza e controllo aziendale faccia la differenza fra un potenziale rischio e un concreto e serio problema.

Il CTU, infine, rinviene diverse tracce di disinstallazioni relative a software di titolarità di Autodesk; si verifica in particolare che le rimozioni sono state effettuate dopo l'inizio delle operazioni peritali e quindi dopo che l'ufficiale giudiziario aveva espressamente comunicato a **α** le ragioni dell'accesso, invitandola formalmente a non effettuare alcuna modifica sui software installati.

Questi comportamenti costituiranno elemento di maggior responsabilità per i soggetti che hanno perpetrato queste azioni e per l'impresa stessa.

Infatti, a seguito dell'accertamento della violazione commessa da **α**, Autodesk instaura un giudizio di merito volto al definitivo accertamento del-

l'illecito, particolarmente grave stante la circostanza dell'avvenuta disinstallazione del software da parte dei dipendenti.

Con questa azione, Autodesk si prefigge di inibire a α la prosecuzione dell'illecito ai sensi della legge sul diritto d'autore (L. 633/1941, art. 156) e ottenere un risarcimento per il danno subito, che viene stimato nella misura di euro 730.000 (danno patrimoniale + danno non patrimoniale), con contestuale cancellazione dei programmi illecitamente duplicati (art. 158) e pubblicazione della sentenza (art. 166).

Nel procedimento emerge inoltre che la duplicazione senza licenza di programmi per elaboratore integra anche il reato ai sensi dell'art. 171 bis[10], ricorrendo lo scopo di profitto. La disinstallazione degli stessi per sottrarli alla descrizione potrebbe inoltre integrare il reato di cui all'art. 388 del Codice Penale, mentre la detenzione di programmi atti ad eludere le misure tecnologiche di protezione sul software potrebbe integrare il reato di cui all'art. 171ter, lett. f) bis[11].

La società α, messa di fronte a questa situazione e preoccupata delle possibili gravi conseguenze della propria condotta, decide di concludere un accordo con Autodesk al fine di porre termine al procedimento di merito.

L'accordo viene stipulato due settimane dopo l'esecuzione della descrizione e prevede l'impegno di α ad acquistare software per un totale di euro 250.000 oltre al pagamento di una ulteriore somma, pari a euro 98.000, a titolo di risarcimento danni e spese.

Ogni copia illecita verrà quindi rimossa e mai più usata, mentre la società inizia il proprio percorso di riorganizzazione e controllo del rischio, con una maggior attenzione alla gestione del proprio software.

**10** Ai sensi dell'art. 171 bis della L. 633/1941 "chiunque abusivamente duplica, per trarne profitto, programmi per elaboratore o ai medesimi fini importa, distribuisce, vende, detiene a scopo commerciale o imprenditoriale o concede in locazione programmi contenuti in supporti non contrassegnati dalla Società italiana degli autori ed editori (SIAE), è soggetto alla pena della reclusione da sei mesi a tre anni e della multa da euro 2.582 a euro 15.493 (...)".

**11** Ai sensi dell'art. 171 ter, lett. f) bis della L. 633/1941 "è punito, se il fatto è commesso per uso non personale, con la reclusione da sei mesi a tre anni e con la multa da euro 2.582 a euro 15.493 chiunque a fini di lucro (...) fabbrica, importa, distribuisce, vende, noleggia, cede a qualsiasi titolo, pubblicizza per la vendita o il noleggio, o detiene per scopi commerciali, attrezzature, prodotti o componenti ovvero presta servizi che abbiano la prevalente finalità o l'uso commerciale di eludere efficaci misure tecnologiche di cui all'art. 102-quater ovvero siano principalmente progettati, prodotti, adattati o realizzati con la finalità di rendere possibile o facilitare l'elusione di predette misure.
Fra le misure tecnologiche sono comprese quelle applicate, o che residuano, a seguito della rimozione delle misure medesime conseguentemente a iniziativa volontaria dei titolari dei diritti o ad accordi tra questi ultimi e i beneficiari di eccezioni, ovvero a seguito di esecuzione di provvedimenti dell'autorità amministrativa o giurisdizionale (...)".

## 4.2 L'illecito nell'impresa ed il rischio sicurezza informatica

È interesse generale che il fenomeno dell'illecito sia efficacemente contrastato, soprattutto quando favorisce **effetti distorsivi per la concorrenza**. I prodotti programma sono infatti elementi d'investimento per le aziende: concorrono alla generazione del valore, attraverso nuove capacità operative e funzionali, e rappresentano una voce di spesa nel conto economico, influenzando di conseguenza gli utili d'esercizio.

Gestire le proprie infrastrutture IT con prodotti software per cui non vengono pagate le licenze d'uso, purtroppo, può diventare una tentazione per chi deve comprimere i costi e aumentare la competitività.

Tuttavia, strategie di questo tipo, oltre a danneggiare i titolari del diritto e ad alterare i mercati, sono **varchi rilevanti per la sicurezza informatica dell'impresa**, con rischi effettivi anche per tutti gli attori che con questa interagiscono.

Ne è esempio questo secondo caso in cui BSA riceve una segnalazione relativa al presunto utilizzo senza licenza di copie di programmi software di titolarità di propri associati presso β, una società che si occupa di produzione e vendita di macchine escavatrici nell'area geografica del Centro Italia.

Anche in questo caso, sommarie informazioni consentono di rilevare che β utilizzerebbe numerosi programmi software, mentre le registrazioni amministrative ed i dati di gestione post-vendita dei prodotti rilevati presso le società produttrici di software interessate non mostrano alcuna informazione circa l'impresa β e prodotti presso questa installati, denotando una probabile situazione di irregolarità.

Nel marzo 2009, BSA incarica il suo studio legale di fiducia di depositare in nome e per conto della suddetta società un ricorso avanti il Tribunale competente, Sezione specializzata in materia di proprietà industriale e intellettuale, al fine di richiedere, come nel caso precedente, un provvedimento che autorizzi la descrizione, l'accertamento e la perizia dei programmi per elaboratore di sua titolarità ed utilizzati da β e, in questo modo, di verificare la corrispondenza fra i programmi per elaboratore utilizzati da β e le licenze d'uso concesse dal titolare dei diritti.

Il provvedimento viene rapidamente promosso dal Tribunale ed eseguito dopo solo 20 giorni dalla richiesta. Trattandosi di procedimenti legali, le modalità attuative ricalcano quelle già esposte nel caso procedente.

L'ufficiale giudiziario, assistito dal perito tecnico nominato dal Tribunale (CTU), oltre che da rappresentanti legali e tecnici della BSA stessa, entra nella sede dell'impresa e convoca il legale rappresentante di β, al quale notifica il provvedimento del Tribunale.

Illustrate le ragioni dell'intervento, richiede all'azienda che il CTU tecnico abbia accesso a tutti i computer e supporti informatici presenti nella sede, con la conseguenza dell'interruzione dell'attività lavorativa da parte dei dipendenti.

Le operazioni di descrizione e rilievo proseguono per circa 5 ore e al termine delle stesse vengono rinvenuti oltre 100 programmi di titolarità di Microsoft e Autodesk (principalmente, programmi Autodesk AutoCAD in varie versioni nonché Microsoft Windows e Office), su un ampio parco di 58 computer e 8 server presenti presso β, per un valore di circa euro 150.000.

Sollecitata dall'ufficiale giudiziario, l'azienda non è in grado di esibire alcuna licenza d'uso e viene dunque alla luce l'illecito commesso, che, in questo caso, colpisce per più di un motivo.

In primo luogo, l'ampia presenza di software non licenziato o di dubbia provenienza in uso anche sui dispositivi server aziendali è elemento di particolare pericolosità; non va infatti sottovalutato il rischio della sicurezza informatica indotto dalla continuità delle infrastrutture telematiche, non solo per l'azienda stessa, ma anche per tutti i soggetti (clienti, fornitori) che con questa sostengono interattività operativa attraverso i sistemi informatici.

In secondo luogo, il numero dei computer positivi al fenomeno e la tipologia dei prodotti illecitamente utilizzati (che vanno dal software operativo di base al prodotto programma specialistico) sono evidenze incontestabili di una grave responsabilità dell'impresa e di una gestione particolarmente spregiudicata del software come fattore produttivo.

A conferma di ciò, si osservi che anche in questo caso vengono rinvenute tracce di disinstallazioni effettuate dopo l'inizio delle operazioni peritali, ovvero dopo che all'azienda era stato richiesto dall'ufficiale giudiziario di non alterare la situazione.

Emerge inoltre che la maggior parte dei programmi erano stati illecitamente scaricati da Internet, confermando la rete come canale telematico per l'acquisizione primaria di prodotti illeciti e, di conseguenza, come strumento da disciplinare con particolare attenzione nel suo uso aziendale.

Gli elementi evidenziati nelle operazioni di accertamento costituiscono le premesse per la promozione di un giudizio di merito da parte di Microsoft e Autodesk, che infatti decidono di muoversi in questa direzione con l'obiettivo di far condannare β al risarcimento di un danno di euro 260.000 (danno patrimoniale + danno non patrimoniale) e di ottenere la contestuale cancellazione dei programmi illecitamente duplicati, nonché la pubblicazione della sentenza.

Anche questa vicenda, tuttavia, si concluderà senza giungere in giudizio grazie a un accordo tra le parti.

Di fronte alla gravità degli illeciti commessi, la società β ritiene infatti più opportuno cercare di evitare il procedimento di merito instaurato avanti il Tribunale e, quattro mesi dopo l'accertamento, concorda con Autodesk e Microsoft l'acquisto di software regolarmente licenziato per un totale di euro 35.000, più il pagamento di euro 80.000 a titolo di risarcimento.

Sostanzialmente l'accordo transattivo evita all'impresa un giudizio e consente un ripristino delle infrastrutture informatiche esistenti, che in questo caso verranno ricondotte progressivamente alla ordinaria operatività con la corretta installazione delle copie autentiche dei prodotti.

## 4.3 Quando le società “resistono”

In questo paragrafo vengono presentate due ulteriori vicende che, a differenza di quelle precedenti, non troveranno una soluzione negoziale, con conseguenze assai più gravi per le aziende coinvolte.

In entrambi i casi il motore dell’iniziativa è ancora BSA, che agisce per tutelare gli interessi delle società produttrici di software ad essa associate e, a fronte del sospetto di violazioni delle norme a tutela dei diritti d’autore sul software, si fa promotrice delle relative azioni di accertamento.

Nel primo caso l’azione viene promossa nei riguardi di una società, γ, che si occupa di costruzione, di impianti di trasporto, di distribuzione e di utilizzazione di energia elettrica nel Nord Italia; le software house interessate sono Adobe, Autodesk e Microsoft.

Nel secondo caso l’azienda oggetto del provvedimento è un Ospedale Civile, mentre le software house sono Adobe, Autodesk, Microsoft e Symantec.

Le iniziative di accertamento promosse da BSA nei confronti di entrambe le aziende si svolgono secondo le modalità previste della legge e già descritte in precedenza: viene richiesta e ottenuta l’autorizzazione dell’autorità giudiziaria competente; in breve tempo l’ufficiale giudiziario, assistito dal perito tecnico nominato dal Tribunale (CTU), oltre che da rappresentanti legali e tecnici di BSA, esegue l’accertamento presso le sedi delle aziende in questione.

Presso l’azienda γ vengono rinvenuti 99 programmi di titolarità di Microsoft (Windows, Office e Project in varie versioni), 31 programmi di titolarità di Autodesk (Autodesk AutoCAD in varie versioni) e 2 programmi di titolarità di Adobe (Macromedia e Acrobat), per un valore di circa euro 43.000, senza che la società possa esibire le licenze relative.

Su questa base Adobe, Autodesk e Microsoft, nel maggio 2002, decidono di instaurare un giudizio di merito presso il Tribunale; la società γ reagisce alla situazione decidendo di costituirsi in giudizio e chiedendo il rigetto delle domande di Adobe, Autodesk e Microsoft.

Questa azzardata decisione, tuttavia, non porterà agli esiti auspicati, anche perché l’illecito commesso risulta chiaramente documentato dal verbale della procedura di accertamento. Il Tribunale, infatti, alla conclusione del procedimento di merito, riconoscerà γ colpevole di aver riprodotto

programmi senza licenza in violazione degli artt. 1 e 64 della L. 633/1941 e la condannerà al pagamento di euro 43.000 a titolo di risarcimento danni e di euro 14.000 per le spese legali.

Nel caso dell'Ospedale Civile, la procedura di accertamento dell'illecito promossa da BSA ed eseguita con particolare celerità dalle autorità giudiziarie porta a rinvenire 96 programmi di titolarità di Microsoft (Windows, Office e Exchange in varie versioni), 1 programma di titolarità di Autodesk (AutoCAD LT 97), 6 programmi di titolarità di Adobe (Photoshop e Acrobat) e 2 programmi Symantec (Norton e Commander) installati su 106 computer, 14 terminali e 15 macchine di laboratorio, per un valore di circa lire 98.878.000[12].

Sulla base di queste evidenze, nell'ottobre 1998 Adobe, Autodesk, Microsoft e Symantec instaurano un giudizio di merito avanti il Tribunale competente, volto al definitivo accertamento dell'illecito, oltre che al fine di inibire all'Ospedale Civile la prosecuzione dell'illecito e ottenere un risarcimento danno in misura non inferiore a lire 100.000.000 (danno patrimoniale + danno non patrimoniale).

Come nel precdente caso, nel tentativo di attuare una strategia di difesa legale, l'Ospedale Civile si costituisce in giudizio, chiedendo il rigetto delle domande di Adobe, Autodesk, Microsoft e Symantec.

E ancora una volta, in ragione degli accertamenti svolti e delle prove raccolte, il Tribunale darà ragione alle società produttrici di software. L'Ospedale Civile viene riconosciuto responsabile della riproduzione dei programmi non licenziati e dovrà risarcire le società titolari dei diritti d'autore per lire 198.000.000, nonché farsi carico delle spese legali per ulteriori lire 17.000.000.

Come si vede, il Tribunale ha ritenuto di dover condannare il convenuto non solo al pagamento dei danni patrimoniali (corrispondenti al prezzo di mercato dei programmi rinvenuti senza licenza) ma anche al pagamento dei danni non patrimoniali, quantificati in una somma equivalente ai danni patrimoniali (euro 98.878.000).

**12** Euro 51.000.

## 4.4 Accertamento dell'autorità di polizia economia e illecito

Quando l'accertamento è a seguito di una azione diretta dell'autorità di polizia economica e tributaria e non a seguito di iniziative legali di parte, come nei casi precedenti, la situazione assume connotati e prospettive diverse. È quanto avviene nei tre casi seguenti.

È il giugno 2007 quando alcuni militari della Guardia di Finanza, unitamente ad un esperto di computer quale ausiliario delle indagini, si recano presso lo studio professionale δ di Firenze per controlli a tutela delle disposizioni di legge sulla protezione del diritto d'autore.

Nel corso dell'ispezione vengono rinvenuti alcuni computer che, per le dichiarazione rese ai militari dal personale, nonché per i successivi accertamenti amministrativi sulla documentazione contabile, risultano essere di proprietà della stessa δ.

Nel corso dell'ispezione viene riscontrata l'avvenuta installazione sui pc esaminati di circa 18 programmi software di titolarità di note società, facenti per altro parte dell'associazione antipirateria BSA, che vengono ritenuti illecitamente riprodotti o, comunque, non lecitamente posseduti in quanto mancanti della documentazione attestante la regolare acquisizione.

La Guardia di Finanza contesta quindi ai legali rappresentanti di δ, Tizio, Caio e Sempronio, il reato di detenzione di prodotti software a scopo imprenditoriale previsto all'art. 171 bis comma 1 della L. 633/1941, sequestrando quindi i computer contenenti programmi illeciti e procedendo alla notifica delle sanzioni pecuniarie e amministrative prescritte.

Diversamente dai casi precedentemente descritti, benché la dimensione dell'illecito e del danno sia meno consistente, l'accertamento da parte dell'autorità di polizia economica porta inesorabilmente all'azione penale e a sanzioni sussidiarie che hanno immediato impatto sull'operatività dell'impresa.

Infatti, a seguito dello svolgimento delle indagini preliminari, Tizio, Caio e Sempronio vengono rinviati a giudizio con decreto del 28 marzo 2008 per il reato previsto all'art. 171 bis comma 1 della L. 633/1941, che prevede la pena della reclusione da sei mesi a tre anni e la multa da euro 2.582 a euro 15.493.

Nel procedimento penale risultano quali parti offese le società di software,

in quanto titolari dei diritti d'autore; esse hanno diritto e interesse a chiedere il risarcimento dei danni subiti sia in sede di procedimento penale, sia - alternativamente - in sede di procedimento civile.

Tizio, Caio e Sempronio richiedono ed ottengono il patteggiamento della pena nel febbraio 2009, a seguito dell'intervenuta parziale riparazione del danno alle società di software, attuata tramite pagamento di euro 5.000. Il patteggiamento, ovvero l'esplicita ammissione del reato e delle relative responsabilità soggettive da parte degli imputati, porterà comunque ad una condanna penale degli amministratori.

Con analoga modalità di accertamento e con le medesime finalità, si è svolto anche il seguente caso, in cui alcuni militari della Guardia di Finanza, unitamente ad un esperto di computer quale ausiliario delle indagini, si recano presso uno studio di architettura, al 4° piano di un prestigioso edificio a Torino, al fine di verificare il lecito utilizzo del software.

Espletate le modalità di rito, ovvero individuati i responsabili dello studio e motivata la loro presenza, la Guardia di Finanza procede al normale controllo dei software in uso all'azienda: la prassi, in questo tipo di controlli, prevede che il tecnico nominato ausiliare di Polizia Giudiziaria dai militari operanti effettui una verifica su tutti i computer aziendali per rilevare tutti i software commerciali installati; dopo questa verifica si procede al controllo documentale delle licenze (quindi viene richiesto che i titolari esibiscano i contratti di licenza e le relative fatture di acquisto). Le licenze devono ovviamente corrispondere al software installato, sia per tipologia che per quantità.

L'ufficio presenta circa 15 postazioni informatiche, suddivise in tre grandi open space, nonché svariate attrezzature anche di costo rilevante, come plotter, stampanti laser a colori ad alta capacità e, più in generale, un arredamento particolarmente ricercato.

La quasi totalità delle postazioni presenta installazioni di software normalmente rilevabile in società operanti nel campo dell'architettura (Autocad, software di disegno di software house quali Adobe e Corel, altro software di progettazione, ecc.), nonché normali software ad uso ufficio quali Microsoft Office, sistemi operativi Microsoft Windows e altri applicativi di vario genere. Vi sono infine installate alcune utilità come WinZip e WinRar e applicazioni non strettamente correlate all'attività, come Google Earth Pro. I primi "campanelli d'allarme" sono proprio WinZip e WinRar, i quali

risultano tutti registrati mediante lo stesso nome e lo stesso numero seriale.

Durante le operazioni di controllo, come da normale procedura, viene anche verificato il registro delle attività di Windows, nei cui "log" risultano tracce della disinstallazione di alcuni software, tra i quali WinZip e Google Earth Pro, disinstallazione avvenuta pochi minuti dopo l'inizio dei controlli. In attesa di valutare se tale attività sia stata compiuta anche su altri terminali, il personale presente al momento del controllo viene allontanato dalle postazioni e raggruppato in un'area dell'ufficio, alla costante presenza di personale militare.

Rilevato che tale cancellazione riguarda un solo terminale, viene individuato il normale utilizzatore della postazione, il quale dapprima nega di aver cancellato alcunché. Vengono quindi ascoltati, singolarmente, tutti i dipendenti dell'azienda, alcuni dei quali confermano di aver chiaramente visto il loro collega mentre procedeva alla disinstallazione dei software. Messo di fronte all'evidenza, il dipendente ammette innanzi ai militari della Guardia di Finanza di aver cancellato i software in quanto privi di regolare licenza. Anche il controllo documentale sul resto dei computer aziendali fa emergere diverse irregolarità, dato che oltre il 70% delle licenze mancano.

I militari procedono quindi alla verbalizzazione, segnalando all'Autorità Giudiziaria il titolare dello studio per violazione dell'art. 171 bis della legge sul diritto d'autore. Inoltre, per la medesima violazione comminano al titolare una sanzione amministrativa pari al doppio del valore del software privo di licenza (nel caso specifico la sanzione supera i 100.000 euro).

Viene quindi attivata l'azione giudiziaria in cui il titolare dello studio verrà imputato per i reati appena descritti. Durante il procedimento, che si instaurerà presso il Tribunale competente, compariranno quali parti offese le aziende titolari dei diritti d'autore, rivalendosi per i danni subiti.

Infine, il dipendente che ha cercato di far sparire i programmi illeciti dalla propria postazione di lavoro viene segnalato dai militari all'Autorità Giudiziaria per una serie di reati: favoreggiamento, intralcio alle indagini e distruzione di materiale probatorio, reati che possono comportare pene molto pesanti.

Concludiamo questa rassegna con un ultimo caso relativo al territorio milanese: nel settembre 2007 viene effettuato un controllo mirato ad accer-

tare reati relativi alla duplicazione abusiva del software nelle imprese, in società e studi professionali operanti nei Comuni di Melegnano, San Giuliano Milanese e San Donato Milanese.

Nel corso dei sopralluoghi la Guardia di Finanza deputata alle verifiche riscontra che almeno la metà delle società controllate fa uso di software illecitamente duplicato o comunque installato al di fuori dei regolari contratti di licenza. Vengono quindi sequestrati 63 computer e 172 programmi informatici illegali. Quest'ultimi con valore commerciale di circa euro 330.000.

Nel corso dell'operazione vengono inoltre rinvenuti nei computer un migliaio di file musicali in formato MP3 illecitamente duplicati.

Alla fine degli accertamenti, quattro responsabili di altrettante aziende sono denunciati all'Autorità Giudiziaria e verranno quindi rinviati a giudizio per il reato di cui all'art. 171 bis.

In tutti i casi di violazione della legge sul diritto d'autore – oltre alla segnalazione per l'avvio dei procedimenti penali - ai titolari delle imprese viene contestata una sanzione amministrativa pari al doppio del prezzo di mercato del software illegalmente utilizzato, ovvero 660.000 euro complessivi. Per gli utilizzatori dei computer aziendali su cui sono risultate installate copie dei file musicali, vengono inoltre contestate sanzioni amministrative proporzionali all'illecito.

In questo caso, un'operazione con obiettivi puramente "geolocati" che entrano nel controllo ordinario di soggetti giuridici presenti sul territorio e che porta a queste evidenze, è un segnale forte che conferma in modo fattuale quanto possa essere reale il rischio discusso in questa pubblicazione.

### Cosa suggeriamo di fare

- ☑ Non autorizzate l'uso di computer di proprietà del personale o di terzi in azienda
- ☑ Non autorizzate la detenzione presso l'azienda di supporti digitali contenenti copie di prodotti coperti da diritto d'autore, salvo esplicita e diretta deroga del responsabile software
- ☑ Richiedete la registrazione in ingresso presso la reception o la segreteria dei dispositivi informatici personali che eventualmente dovessere essere detenuti anche temporaneamente (mai fatti funzionare o collegati alla rete) all'interno dell'azienda per particolari esigenze individuali
- ☑ All'atto della registrazione del materiale, fornite copia cartacea delle istruzioni in vigore con divieti e norme da seguire in azienda
- ☑ Richiedete la sottoscrizione per presa visione delle norme e tenetene una copia in archivio presso la reception/segreteria
- ☑ Il materiale informatico deve essere sempre formalmente assegnato ai dipendenti
- ☑ Abbiate sempre l'inventario aggiornato dei dispositivi informatici di proprietà dell'impresa, dei verbale di consegna e lista dei prodotti autorizzati ed installati sui computer
- ☑ Imballi, documenti di licenza, supporti di memorizzazione devono essere custoditi attentamente

# 5. LA GESTIONE DEL PROBLEMA IN AZIENDA: LE POSSIBILI AZIONI DI CONTENIMENTO DEL RISCHIO E MITIGAZIONE DEL DANNO

## 5.1 I principi generali da seguire

Ridurre al minimo i rischi legati all'uso illecito di software sulle piattaforme informatiche in azienda è un obiettivo che la direzione d'impresa deve attuare per garantire la propria sicurezza informatica e per minimizzare il rischio di vedersi imputate responsabilità amministrative e penali.

Il percorso non può essere né semplice né immediato. Non si tratta, infatti, di porre in atto un'azione "impositiva" dell'impresa, bensì di generare e far condividere a tutta l'organizzazione aziendale una consapevolezza e un insieme di valori.

È essenziale capire lo stato dei fatti, la situazione reale in cui l'impresa oggettivamente si trova rispetto al problema; predisporre delle norme interne di contrasto del problema; decidere l'organizzazione delle risorse da impegnare nelle attività di controllo; fare idonea formazione e informazione per tutti i lavoratori.

L'azienda che intenda strutturarsi per affrontare correttamente il rischio, invece di subirlo, dovrà in particolare affrontare i seguenti sei passaggi.

**1** Coinvolgere e responsabilizzare il proprio personale

L'attuale livello di diffusione dell'ICT e dei dispositivi informatici nelle piccole e medie imprese rende necessario che comportamenti idonei a evitare i rischi legati alla violazione delle leggi sul diritto d'autore siano compresi e adottati da tutti i dipendenti.

Questo presuppone che vi sia un'efficace politica di comunicazione ed informazione sulle norme a cui il dipendente dovrà attenersi anche in considerazione del rispetto del contratto di lavoro e degli obblighi di legge.

L'esperienza insegna che comportamenti disciplinati sono ottenuti quando il rischio ed il problema sono percepiti e correttamente compresi dal personale.

A questo riguardo può essere utile prevedere alcuni momenti di incontro interni, nonché la realizzazione di un opportuno materiale informativo e formativo che spieghi il rischio e illustri le politiche e le norme che si vogliono attuare.

Opportuno (e fortemente suggerito) è che ogni nuovo assunto, collaboratore diretto o fornitore riceva una formale informazione sulla tematica, sulle regole comportamentali e sulle prescrizioni aziendali da attuare e sottoscriva di essere stato raggiunto da tale informazione.

**2** Definire le corrette politiche di sicurezza per il software usato in azienda, predisporre norme e istruzioni al personale

È indispensabile che le norme e le istruzioni predisposte per dipendenti e collaboratori siano chiare e rigorose: devono stabilire essenzialmente e senza alcuna possibilità di equivoco ciò che è consentito e ciò che non lo è.

Questo dipende direttamente dalle scelte fatte specificatamente sull'uso corretto delle infrastrutture digitali e sulla loro sicurezza.

Una robusta normativa aziendale, proposta all'interno degli strumenti ordinari di controllo (es. Codice disciplinare), deve essere capace di mettere in chiaro quali comportamenti individuali possano essere accettati e leciti, quali, invece, oltre ad essere disciplinarmente contestabili, debbano essere sostanzialmente separati dal volere dell'azienda e letti quali azioni individuali e soggettive.

Può essere opportuno investire in un eventuale supporto tecnico e legale sia per poter compiere scelte tecniche e strutturali (es. consentire l'uso di dispositivi informatici personali in azienda), sia per predisporre norme comportamentali corrette anche sotto il profilo giuslavoristico (es. comportamenti vietati da inserire nel Codice disciplinare).

A partire da queste prime scelte strutturali, con il contributo delle competenze aziendali opportune (es. Dir. Personale, Responsabile IT, ecc.) si potranno predisporre le istruzioni formali e vincolanti che guideranno i comportamenti individuali nell'uso delle dotazioni e infrastrutture telematiche, fornendo fra l'altro il quadro normativo circa gli obblighi e i divieti da adottare. Durante eventuali controlli o ispezioni, questi elementi costituiranno la documentazione rilevante circa i comportamenti richiesti al personale e quindi definiranno eventuali responsabilità per gli illeciti rilevati.

**3** Nominare un responsabile per le risorse software

La corretta gestione delle risorse coperte da licenza d'uso deve essere oggetto delle responsabilità di un incaricato aziendale che monitorerà

l'impiego di questi prodotti in tutto il ciclo produttivo d'impresa: dalle fasi di selezione e acquisto (in cui vengono indirettamente acquisiti anche gli obblighi contrattuali d'uso) alla registrazione e all'assegnazione in azienda del prodotto, dal controllo periodico del corretto uso in termini di liceità alla dismissione o al rinnovo tecnologico.

Tutte queste attività dovrebbero essere assegnate a un unico responsabile aziendale, selezionato soprattutto per le proprie competenze e attitudini. Rendere espliciti mansioni, poteri e responsabilità di questo incaricato potrà inoltre comunicare agli altri lavoratori un sistema di valori e un preciso segnale di attenzione al rischio informatico e alla sua gestione.

### 4 Effettuare ogni anno un inventario delle risorse digitali

L'inventario "fisico", e non solamente contabile, deve essere considerato un'attività fondamentale e prioritaria. Va precisato che deve essere eseguito sia per valutare le potenziali esposizioni, sia per riconciliare in modo contabile le risorse software lecitamente acquisite dall'impresa, identificando il prodotto, la documentazione amministrativa e contabile, le chiavi di identificazione, l'assegnatario o chi ne abbia regolare uso.

Prodotti ad uso generale, come ad esempio informatica di reparto o d'ufficio non assegnata a singoli utilizzatori, dovranno essere comunque oggetto di responsabilità di un preciso incaricato, di norma il manager/coordinatore.

Eventuali discrepanze inventariali dovranno evidentemente essere sistemate, mentre le informazioni raccolte costituiranno l'archivio di base dell'installato e degli utilizzatori.

Sul mercato sono disponibili prodotti e soluzioni informatiche che consentono, in modo più o meno complesso a seconda della dimensione dell'infrastruttura informatica aziendale, di automatizzare il controllo, il monitoraggio e la gestione inventariale del software aziendale.

### 5 Accentrare l'acquisto e la distribuzione interna del software

I prodotti digitali dovrebbero essere selezionati e comprati tramite un'unica funzione responsabile degli acquisti, che ne curerà tutti gli aspetti, come ad esempio la valutazione degli obblighi inerenti la licenza d'uso, la dimostrazione di liceità dell'acquisto e di originalità della copia disponibile sul supporto originale.

Una volta in azienda, il prodotto verrà trasferito al responsabile di cui al punto 3, che provvederà alla sua assegnazione al singolo dipendente e alla sua registrazione.

La documentazione amministrativa e fiscale di acquisto, il relativo contratto e quella interna, come ad esempio i moduli di assegnazione, dovranno essere conservati per tutta la durata di permanenza in azienda del prodotto.

È consigliabile inoltre che sia facilmente reperibile e consultabile in caso di ispezione o controllo da parte degli organi preposti.

### 6 Effettuare controlli e verifiche periodiche circa il corretto uso delle risorse informatiche

In supporto alle responsabilità soggettive e individuali, l'impresa dovrebbe prevedere alcune procedure formali di controllo, in modo che le risorse software siano gestite, protette e utilizzate efficacemente, efficientemente e lecitamente.

I verbali di questi controlli devono essere conservati con cura, perché possono essere esibiti in caso di ispezioni, a dimostrazione dell'adesione puntuale dell'azienda agli obblighi di legge.

Appositi prodotti, meglio noti come soluzioni appplicative di *Assets Management* possono rendere queste attività automatiche, non gestite quindi da personale, ma eseguite autonomamente dal sistema informatico aziendale, che provvederà ad identificare eventuali discrepanze inventariali e a comunicare al dipendente e al suo responsabile le eventuali anomalie.

## 5.2 Le norme e le istruzioni interne da applicare

Definita la strategia d'uso e di protezione del software e delle risorse digitali, è necessario predisporre ed emettere le fondamentali norme aziendali e le relative istruzioni attuative per il personale.

Le sei istruzioni presentate di seguito possono assicurare un grado minimo di protezione dell'azienda.

**1** Utilizzo personale/a scopo di lavoro di strumenti informatici aziendali assegnati ai dipendenti

L'istruzione ha come obiettivo la regolamentazione dell'utilizzo per uso personale degli strumenti informatici aziendali, ossia dovrà definire in modo puntuale le regole e i confini da non superare nell'uso delle dotazioni.

L'impresa dovrebbe indicare se e con quali modalità è concesso l'uso personale (che comunque deve essere sempre marginale) delle dotazioni informatiche e delle applicazioni (posta elettronica, accessi Internet). Nel caso di dotazioni informatiche mobili (personal computer portatili) l'istruzione dovrà specificare se ne è consentito l'uso presso l'abitazione o altri luoghi. Per contro dovrà anche stabilire se è permesso l'uso in ufficio di dotazioni informatiche dei dipendenti.

A titolo d'esempio, dovrebbero essere specificate norme tecniche e comportamentali circa:

- la connessione fisica e logica[13] alla rete aziendale (es. uso wifi in aree pubbliche);
- l'accesso alla rete Internet e a siti web (es. siti di scommesse e giochi);
- l'uso di protocolli di comunicazione (es. P2P);
- il download di materiale (es. prodotti multimediali);
- l'installazione di prodotti software (es. shareware o freeware);
- l'installazione di device aggiuntivi (es. hard disk esterni);
- le modifiche alle configurazioni standard (es. blocco funzioni di firewall).

Tenuto conto delle Linee guida sulla disciplina della navigazione in Internet e sulla gestione della posta elettronica nei luoghi di lavoro emanate dal Garante per la Privacy, con propria deliberazione n. 13 del 1 marzo 2007, i dipendenti e/o collaboratori dovrebbero attenersi alle seguenti istruzioni e raccomandazioni nell'utilizzo del personal computer.

**13** Per connessione fisica si intende l'accesso al cavo di rete o alla risorsa wifi dal computer, mentre per connessione logica, il logon da un dispositivo informatico, già connesso alla rete fisica, alla applicazione in rete.

- Il personal computer con i relativi programmi, il telefono, i fax e ogni altro bene aziendale costituiscono strumenti di lavoro il cui utilizzo ricade sotto la responsabilità dell'azienda stessa, che li mette a disposizione dei propri dipendenti a condizione che vengano custoditi con cura dal dipendente cui sono assegnati, evitando manomissioni, danneggiamenti o utilizzi, anche da parte di altre persone, per scopi non consentiti.
- Non è consentito modificare le configurazioni impostate sul proprio PC né procedere ad installare dispositivi di memorizzazione, comunicazione o altro (come, ad esempio, masterizzatori, modem, ecc.).
- Sui personal computer dotati di scheda audio e/o di lettore CD non è consentito l'ascolto di programmi, file audio o musicali, se non a fini prettamente lavorativi.
- Il personal computer deve essere protetto da password di accensione, che deve essere attivata anche per il disco fisso. Lo screensaver deve essere impostato per tempi brevi (15 minuti) e, quando attivato, disinseribile solo tramite password utente.
- Il personal computer deve essere spento ogni sera prima di lasciare gli uffici e in caso di assenze prolungate dall'ufficio o in caso di suo inutilizzo. In ogni caso, lasciare un elaboratore incustodito connesso alla rete può essere causa di utilizzo da parte di terzi, senza che vi sia la possibilità di provarne in seguito l'indebito uso.
- Non è consentito utilizzare programmi diversi da quelli ufficialmente installati dalla azienda né installare autonomamente programmi provenienti dall'esterno, sussistendo infatti il grave pericolo di introdurre virus informatici e/o di alterare la funzionalità delle applicazioni software esistenti.
- Non è consentito scaricare file contenuti in supporti magnetici/ottici non aventi alcuna attinenza con la propria prestazione lavorativa.
- Tutti i file di provenienza incerta o esterna, ancorché attinenti all'attività lavorativa, devono essere sottoposti al controllo e relativa autorizzazione all'utilizzo da parte della Direzione o persona delegata.
- Ogni utente deve prestare la massima attenzione ai supporti di origine esterna, avvertendo immediatamente il personale addetto nel caso in cui siano rilevati virus e seguendo le procedure di protezione antivirus.
- Tutti i supporti magnetici rimovibili (dischetti, CD e DVD riscrivibili, supporti USB, ecc.), contenenti dati sensibili nonché informazioni costituenti know-how aziendale, devono essere trattati con partico-

lare cautela, onde evitare che il loro contenuto possa essere trafugato o alterato e/o distrutto o, successivamente alla cancellazione, recuperato.
- Al fine di assicurare la distruzione e/o inutilizzabilità di supporti magnetici rimovibili contenenti dati sensibili, ciascun utente dovrà contattare il personale addetto e seguire le istruzioni da questo impartite.
- In ogni caso, i supporti magnetici contenenti dati sensibili devono essere adeguatamente custoditi dagli utenti in armadi chiusi.
- È vietato l'utilizzo di supporti rimovibili personali.
- L'utente è responsabile della custodia dei supporti e dei dati aziendali in essi contenuti.

L'utilizzo degli strumenti informatici di proprietà dell'azienda dovrà essere quindi autorizzato e subordinato a precise condizioni che garantiscano la sicurezza dei dispositivi informatici, delle informazioni contenute e la liceità di ciò che viene fatto.

Va ribadito che la presenza di materiale digitale e informatico di tipo personale aumenta in modo esponenziale il rischio e i costi gestionali, diminuisce l'affidabilità della piattaforma e, soprattutto, rende maggiormente complessa una eventuale azione di controllo e di verifica. Non ultimo, la presenza di dati sensibili personali, quindi protetti dalle norme di legge sulla Data Privacy, impone particolari attenzioni per la gestione del materiale. Questa istruzione dovrà quindi indicare questi elementi con la massima precisione e dettaglio possibile.

Per quanto riguarda l'accesso a Internet da un indirizzo IP della rete aziendale o dai sistemi di posta dell'impresa, l'utilizzo occasionale e sporadico di questi sistemi per uso personale durante o al di fuori del normale orario di lavoro deve essere consentito solo a condizione che siano rispettate precise regole comportamentali. Ogni passaggio nella rete, infatti, verrà attribuito ad una utenza della rete aziendale stessa e, quindi, le attività autonome del dipendente espongono potenzialmente l'impresa.

Per ciò che concerne l'utilizzo della rete aziendale dovrebbero essere specificate nel regolamento aziendale norme tecniche e comportamentali quali, a titolo d'esempio, le seguenti.

- Il personal computer dato in affidamento all'utente permette l'accesso alla rete dell'azienda solo attraverso specifiche credenziali di autenticazione.

- Le credenziali di autenticazione per l'accesso alla rete vengono assegnate dal personale addetto, previa formale richiesta del Responsabile dell'ufficio/area nell'ambito del quale verrà inserito ed andrà ad operare il nuovo utente.
- Le credenziali di autenticazione consistono in un codice per l'identificazione dell'utente (User Id), assegnato dal personale addetto, associato ad una parola chiave (password) riservata che dovrà venir custodita dall'incaricato con la massima diligenza e non divulgata. Non è consentita l'attivazione della password di accensione senza preventiva autorizzazione da parte del personale addetto.
- È necessario procedere alla modifica della parola chiave a cura dell'utente, incaricato del trattamento, al primo utilizzo e, successivamente, almeno ogni sei mesi.
- Qualora la parola chiave dovesse venir sostituita, per decorso del termine sopra previsto e/o in quanto abbia perduto la propria riservatezza, si procederà in tal senso d'intesa con il personale addetto.
- Soggetto preposto alla custodia delle credenziali di autenticazione è il personale incaricato del servizio dall'azienda;
- È assolutamente proibito entrare nella rete e nei programmi con un codice d'identificazione utente diverso da quello assegnato. Le parole chiave d'ingresso alla rete e ai programmi sono segrete e vanno comunicate e gestite secondo le procedure impartite.
- Le unità di rete sono aree di condivisione di informazioni strettamente professionali e non possono, in alcun modo, essere utilizzate per scopi diversi. Pertanto, qualunque file che non sia legato all'attività lavorativa non può essere dislocato, nemmeno per brevi periodi, in queste unità.
- L'azienda si riserva la facoltà di procedere alla rimozione di ogni file o applicazione che riterrà essere pericolosi per la sicurezza del sistema ovvero acquisiti o installati in violazione del presente Regolamento/Codice di condotta.
- Risulta opportuno che, con regolare periodicità (almeno ogni tre mesi), ciascun utente provveda alla pulizia degli archivi, con cancellazione dei file obsoleti o inutili. Particolare attenzione deve essere prestata alla duplicazione dei dati, essendo infatti necessario evitare un'archiviazione ridondante.

Il mancato rispetto dell'istruzione da parte del dipendente potrà essere sanzionato disciplinarmente; l'effetto deterrente di questa possibilità po-

trà anche non essere decisivo nel caso di dipendenti poco leali e comunque orientati ad agire scorrettamente, ma sicuramente l'aver previsto un'istruzione esplicita consentirà all'impresa di affrontare con serenità le eventuali problematiche ingenerate da comportamenti non idonei.

### 2 Divieti espliciti e comportamenti non consentiti nell'uso di dotazioni informatiche

Questa istruzione dovrebbe indicare ed esplicitare ai dipendenti che usano infrastrutture telematiche aziendali il divieto di accedere, scaricare o distribuire materiale digitale che sia potenzialmente illecito (es. programmi software atti a contraffare, copie abusive) o che possa essere considerato inappropriato, offensivo o irrispettoso nei confronti di altri (es. materiali che contengono immagini o descrizioni sessuali esplicite, materiali che patrocinano attività illegali o che propagandano intolleranza verso altri).

È opportuno che questa regola, che può sembrare scontata, venga sempre formalizzata e corredata di indicazioni, le più precise e circoscritte possibili come, a titolo d'esempio, quelle di seguito riportate.

- Non è consentito navigare in siti non attinenti allo svolgimento delle mansioni assegnate, soprattutto in quelli che possono rivelare le opinioni politiche, religiose o sindacali del dipendente.
- Non è consentita l'effettuazione di ogni genere di transazione finanziaria ivi comprese le operazioni di remote banking, acquisti on-line e simili salvo casi direttamente autorizzati dalla Direzione o persona delegata e con il rispetto delle normali procedure di acquisto.
- È vietata ogni forma di registrazione a siti i cui contenuti non siano legati all'attività lavorativa.
- Non è permessa la partecipazione, per motivi non professionali, a forum, l'utilizzo di chat line, di bacheche elettroniche e le registrazioni in guest book, anche utilizzando pseudonimi (o nicknames).
- Non è consentito utilizzare programmi informatici o strumenti per intercettare, falsificare, alterare o sopprimere per finalità illecite il contenuto di comunicazioni e/o documenti informatici.
- Non è consentita la memorizzazione di documenti informatici di natura oltraggiosa e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica.
- Si raccomanda di limitare l'accesso ad Internet, tenendo presente che, salvo casi eccezionali, non è consentito accedere a siti non at-

tinenti allo svolgimento delle mansioni assegnate; è in ogni caso vietato accedere a siti i cui contenuti non siano adeguati alla serietà e al decoro richiesti nei luoghi di lavoro.

### 3 Installazione e uso di prodotti software sulle infrastrutture informatiche aziendali

Ogni dispositivo informatico in assegnazione ai dipendenti deve possedere le adeguate licenze per il software in uso. Queste licenze dovranno risultare presenti a partire dal momento di assegnazione del dispositivo, quando al dipendente verrà chiesto di acquisire formalmente il materiale.

A partire da questo preciso momento, il materiale sarà utilizzato dall'assegnatario, che non deve essere lasciato libero di installare autonomamente prodotti software o altro materiale, se non dopo autorizzazione da parte del coordinatore preposto. Anche se leciti, infatti, questi oggetti potrebbero non essere lecitamente utilizzabili nell'ambito di un contesto aziendale e produttivo. È il caso, ad esempio, dei prodotti di libero utilizzo (freeware o shareware) licenziati esclusivamente per i soli utenti non business.

A titolo d'esempio il regolamento aziendale dovrebbe specificare le seguenti norme tecniche e comportamentali.

- Onde evitare il grave pericolo di introdurre virus informatici nonché di alterare la stabilità delle applicazioni dell'elaboratore, è consentito installare programmi provenienti dall'esterno solo se espressamente autorizzati dalla Direzione o persona delegata.
- Non è consentito l'uso di programmi non distribuiti ufficialmente dalla azienda distributrice (vedere, in proposito, gli obblighi imposti dal D.Lgs. 518/1992 sulla tutela giuridica del software e dalla L. 248/2000, contenente nuove norme di tutela del diritto d'autore).
- Non è consentito lo scarico di software gratuiti (freeware e shareware) prelevati da siti Internet, se non espressamente autorizzato dalla Direzione o persona delegata.

### 4 Uso di prodotti aventi il diritto di riproduzione e proprietà intellettuale

La maggior parte delle informazioni (testi) e dei prodotti digitali (programmi, prodotti audio e video, file di dati, ecc.) ottenibili dalla rete In-

ternet è soggetta al divieto di riproduzione o ad altra protezione prevista dal diritto di proprietà intellettuale.

È indispensabile acquisire correttamente questo materiale e comprenderne tutte le restrizioni sul diritto di riproduzione e uso.

In nessun caso deve essere consentito copiare/duplicare software con licenza o caricare sulla macchina oggetti che in qualche modo dimostrino di essere potenzialmente tutelati da un diritto d'autore, come ad esempio banche dati, prodotti multimediali, libri digitali.

L'istruzione deve assicurare di rispettare tutte le richieste e le limitazioni esplicite connesse con l'uso di tale materiale.

Pertanto, il regolamento aziendale dovrebbe contenere una norma comportamentale esplicita relativa al divieto di riproduzione o duplicazione di programmi informatici ai sensi della L. 128/2004.

### 5 Protezione delle informazioni

Tutte le informazioni e i dati aziendali, compresi quelli relativi alle informazioni amministrative e contrattuali del software presente in azienda, devono essere correttamente protette per garantire che le misure attuate a protezione del rischio della software piracy siano realmente efficaci.

Questa istruzione dovrà regolamentare questi aspetti rilevanti e potrebbe essere formulata nel modo seguente.

- Il sistema informatico di azienda è protetto da software antivirus aggiornato quotidianamente. Ogni utente deve comunque tenere comportamenti tali da ridurre il rischio di attacco al sistema informatico aziendale mediante virus o mediante ogni altro software aggressivo.
- Nel caso il software antivirus rilevi la presenza di un virus, l'utente dovrà immediatamente sospendere ogni elaborazione in corso senza spegnere il computer, nonché segnalare prontamente l'accaduto al personale addetto.
- Ogni dispositivo magnetico di provenienza esterna all'azienda dovrà essere verificato mediante il programma antivirus prima del suo utilizzo e, nel caso venga rilevato un virus, dovrà essere prontamente consegnato al personale addetto. La dispersione di informazioni o la perdita del materiale originale potrebbe infatti costituire un punto

di debolezza anche del processo istituito a protezione e controllo del software.

**6** Accesso dei visitatori o fornitori alla rete informatica aziendale

Al fine di garantire la sicurezza degli ambienti IT in linea con quanto stabilito dalla normativa interna, devono essere disciplinati anche i comportamenti dei visitatori esterni in possesso di dotazioni IT personali (PC portatili o simili), ai quali non potrà essere concesso l'accesso alla rete telematica interna. Questo per evitare sia l'accesso e lo scarico (upload) di materiale in uso all'azienda, che potrebbe essere poi riutilizzato o ridistribuito, sia l'introduzione di prodotti non controllati e quindi potenzialmente illeciti sulla rete aziendale.

## 5.3 Le verifiche ispettive

Ruolo cardine nel contrasto e nella repressione della pirateria intellettuale è svolto dalla Guardia di Finanza, che oltre ai tradizionali compiti di polizia tributaria e giudiziaria ha assunto anche responsabilità nella tutela degli interessi economico-finanziari dello Stato.

Da ultimo, il D.Lgs. 68/2001 ha meglio precisato i compiti relativi alla protezione degli interessi, *latu sensu* definiti finanziari, pubblici. Uno dei comparti (precisamente quello indicato e circoscritto alla lettera L) riguarda la tutela dei diritti di utilizzazione di opere dell'ingegno previsti dalla normativa sul diritto d'autore, i marchi, i brevetti, i modelli e le invenzioni industriali con diritto di sfruttamento economico ed esclusivo.

Per l'adempimento dei propri compiti di controllo e di accertamento, il Corpo è dotato di ampi poteri istruttori e di indagine. Allo scopo di individuare e reprimere le violazioni, i Comandi della Guardia di Finanza possono far effettuare verifiche presso aziende e privati anche per accertamenti in merito alla tutela dei brevetti e dei diritti d'autore, avvalendosi di tutte le facoltà d'indagine tradizionalmente utilizzate per le ispezioni tributarie.

Le attività di polizia economica si svolgono sia in forma preventiva con l'azione di intelligence, di vigilanza tributaria, di controllo delle dogane, sia come repressione degli illeciti attraverso azioni specifiche e mirate. Nel corso degli ultimi anni la Guardia di Finanza ha attivato rapporti diretti di collaborazione sia con l'Autorità per le Garanzie nelle Comunicazioni che con enti e associazioni per la tutela della proprietà intellettuale (oltre alla già citata BSA, anche SIAE[14], INDICAM[15], ecc.), al fine di rendere maggiormente efficace la capacità di rilevazione e discriminazione dell'illecito nel corso degli interventi ispettivi.

L'utilizzo di poteri amministrativi consente di svolgere attività ispettiva di tipo preventivo che è esclusa per la Polizia Giudiziaria, ma con poteri di ampiezza inconsueta per il comparto amministrativo.

Potranno infatti essere eseguiti accessi, anche domiciliari, ricerche documentali, ispezioni e verifiche, nonché accertamenti bancari. In sintesi, potranno essere utilizzati tutti gli strumenti propri della polizia tributaria[16].

Ferme restando le attribuzioni e i compiti demandati ai vari organi della Polizia Giudiziaria dal codice (artt. 55 e segg. C.P.P.) e dalla legislazione speciale, il Ministero dell'Interno ha, con proprio D.M. 28 aprile 2006, di-

**14** SIAE – Società Italiana Autori ed Editori, ente che tutela il diritto d'autore e amministra le opere di più di 85.000 soci aderenti.

**15** INDICAM – Associazione senza fini di lucro costituitasi per il contrasto e la lotta alla contraffazione e che rappresenta più di centottanta imprese nazionali.

**16** A tal proposito deve però evidenziarsi una carenza normativa in ordine ai limiti e garanzie esplicitamente previsti per l'attività di P.T. in materia di "diritti del contribuente" (L. 212/2000). Se infatti può agevolmente dedursi l'applicabilità, in via interpretativa, di molti istituti, non è infatti possibile individuare, ad esempio, un'autorità analoga al "garante del contribuente" da indicare al soggetto controllato per inoltrare le eventuali doglianze circa l'operato della polizia economica. D'altronde non può assumersi esistente una competenza del citato garante per un comparto, la polizia economica, che esula da quello tributario, cioè riferibile alle entrate. Ciò non fa comunque dubitare circa la equiparazione "orizzontale" delle facoltà ispettive in termini di accesso, ispezione e verifica, garantite dagli artt. 32 e 33 del D.P.R. 600/1973 e dagli artt. 51 e 52 del D.P.R.633/1972.

sciplinato il coordinamento tra le varie Forze di Polizia nelle aree di contiguità operativa. Per quanto riguarda il tema in argomento rileva la competenza riconosciuta alla Guardia di Finanza in materia di commercio elettronico, valutaria, della tutela dei marchi, dei brevetti e della proprietà intellettuale.

Anche la Polizia Postale e delle comunicazioni è impegnata in attività di investigazione per la prevenzione e il contrasto alle violazioni sul diritto d'autore, settore in cui è particolarmente evidente la contiguità dell'azione investigativa con le competenze di altre Forze di Polizia e in particolare con quelle rimesse alla Guardia di Finanza dall'art. 2, comma 2, lettera l) del D.Lgs. 68/2001, le quali possono svolgersi anche attraverso il monitoraggio di Internet per individuare le violazioni commesse attraverso la rete.

La Polizia Postale e delle comunicazioni procederà altresì al contrasto degli illeciti concernenti i mezzi di pagamento e il diritto d'autore in tutti i casi in cui l'utilizzo distorto dello strumento informatico o delle tecnologie di rete rappresenti il modo esclusivo o assolutamente prevalente di perpetrazione degli stessi.

Nello svolgimento di questo ruolo, la Polizia Postale si raccorderà con la Guardia di Finanza cui, secondo le esplicite previsioni del D.Lgs. 68/2001, compete gravitare in modo generale sull'area della tutela dei marchi, dei brevetti e della proprietà intellettuale, nonché della tutela dei mezzi di pagamento, ferme restando le attività svolte dal Corpo in favore della Autorità garante per le comunicazioni, per la tutela del diritto d'autore e del regolare pagamento dei canoni di abbonamento al servizio pubblico radiotelevisivo.

In sostanza sarebbero di competenza della Polizia Postale le indagini sul Web, finalizzate a ricercare le violazioni in materia di diritto d'autore. Resta salva la possibilità per le altre Forze di Polizia di sviluppare indagini attraverso la rete che, incidentalmente, conducano ad accertare violazioni della specie. La Guardia di Finanza svolgerà invece indagini classiche nel settore, non escludendo tuttavia sviluppi investigativi sul Web. È comunque evidente una sovrapposizione tra quanto previsto per la Guardia di Finanza in materia di controllo sul commercio elettronico, soprattutto di beni dematerializzati e servizi, e quanto previsto per la Polizia Postale.

Tuttavia, l'unico organo che può utilizzare l'intera gamma dei poteri è la Guardia di Finanza, cui competono tra l'altro anche i poteri previsti per la

Polizia tributaria ed economica e che resta destinataria delle comunicazioni, obbligatorie ex art. 36 del D.P.R. 600/1973, per quanto riguarda i fatti che potrebbero rilevare come violazioni tributarie. Poiché i militari della Guardia di Finanza possono effettuare le verifiche presso i contribuenti, avvalendosi di tutte le facoltà d'indagine tradizionalmente utilizzate per le ispezioni ai fini delle imposte sui redditi e dell'IVA, anche per sviluppare accertamenti nelle altre materie economiche e finanziarie affidate alla loro tutela, allo scopo di individuare e reprimere le violazioni allo sfruttamento dei brevetti e diritti d'autore, i Comandi del Corpo possono attivare, per le finalità descritte, un'ampia serie di potestà d'indagine, ivi comprese le facoltà di:

- procedere all'esecuzione di accessi, ispezioni e verifiche;
- invitare i soggetti che esercitano imprese, arti o professioni a comparire di persona o per mezzo di rappresentanti per esibire documenti o per fornire dati, notizie e chiarimenti;
- inviare questionari;
- invitare qualsiasi soggetto ad esibire o trasmettere, anche in copia fotostatica, documenti e fatture relativi a determinate cessioni di beni o prestazioni di servizi ricevute e a fornire ogni informazione relativa alle operazioni stesse.

### Modalità di esame dei programmi

In conseguenza dell'entrata in vigore della normativa inerente la polizia economica (D.Lgs. 68/2001), la tutela del diritto d'autore assume una valenza non più incidentale rispetto agli altri compiti di servizio. Anche il controllo del software in occasione di accessi, verifiche, ecc., deve ormai ritenersi parte di una procedura standard. L'accertamento della Guardia di Finanza diventa importante anche quando eseguito su computer utilizzati da aziende o da professionisti, allo scopo di verificare l'eventuale presenza sui PC di programmi clonati.

L'accertamento in ogni caso si sostanzia nella ricerca puntuale di tutti i programmi esistenti all'interno dei PC allo scopo di eseguire un inventario e, successivamente, nel confronto tra i programmi installati e le licenze possedute. Dovendosi comparare le licenze d'uso disponibili da parte del soggetto controllato, che individuano il tipo di utilizzo e il numero delle copie concesso allo stesso, relativamente ai programmi per elaboratore, disk, CD-ROM, ecc., dovrà analizzarsi ognuno dei suddetti supporti estranei all'elaboratore.

Dovranno però soprattutto analizzarsi il sistema operativo e il software applicativo. Al numero di programmi installati sui PC dovrà corrispondere un numero uguale di licenze o licenze multiple. Lo stesso vale per ogni disk, CD-ROM, ecc. che sarà rinvenuto nella fase di controllo.

Se il contribuente non dovesse disporre della licenza (per smarrimento, furto, ecc.), la fattura, riportante la dicitura dell'acquisto del software, può essere un valido elemento probatorio, da riscontrare eventualmente con una richiesta al venditore. Per quanto riguarda, invece, il ritrovamento di CD-ROM non originali, si ricorda che la legge prevede che si possa fare una sola copia dell'originale. Infatti l'art. 64 ter della L. 648/2000 recita *"Salvo patto contrario, non sono soggette all'autorizzazione del titolare dei diritti le attività indicate nell'art. 64-bis, lettere a) e b), allorché tali attività sono necessarie per l'uso del programma per elaboratore conformemente alla sua destinazione da parte del legittimo acquirente, inclusa la correzione degli errori"*.

Qualora la Polizia Giudiziaria compisse atti o operazioni che richiedono specifiche competenze tecniche, potrà avvalersi ai sensi dell'art. 348 C.P.P. di persone idonee che non potranno rifiutare la propria opera. Tali soggetti acquisiranno la qualifica di "ausiliari della Polizia Giudiziaria".

Per quanto riguarda i cosiddetti "driver" necessari al corretto funzionamento di dispositivi connessi al personal computer (macchine fotografiche digitali, registratori digitali e quant'altro) il software è da ritenersi di norma autorizzato e il suo uso non costituisce un atto illecito.

Viceversa, nel caso in cui tali "versioni di valutazione" siano state modificate per renderle utilizzabili ("crakkate") ovvero siano stati utilizzati altri software o crack allo scopo di superare le limitazioni del programma stesso, si riscontra un software cosiddetto "pirata". Tecnicamente tale operazione è definita "decompilazione" e rientra nella previsione degli artt. 102 quater e quinquies della Legge sul diritto d'autore. La violazione penale è quella prevista dall'art. 171 bis della legge stessa.

### Accesso e ispezione

Il personale in servizio d'istituto, in virtù dei poteri conferiti dall'art. 2 del D.Lgs. 68/2001, oltreché di eventuali altre specifiche disposizioni di natura tributaria o giudiziaria, **ha facoltà di accedere presso i locali dell'impresa** per eseguirvi controlli a tutela delle disposizioni di legge sulla protezione del diritto d'autore.

Va ricordato che sussiste l'obbligo anche per il personale della Guardia di Finanza, in quanto Forza di Polizia, di qualificarsi compiutamente esibendo le tessere personali di riconoscimento, indicando inoltre lo scopo della visita, che deve essere espressa nell'apposito foglio di servizio.

Gli ispettori avranno necessità di prendere contatto con gli idonei interlocutori nell'impresa ovvero coloro che avendo ordinarie procure o ricoprendo incarichi direttivi saranno i referenti formali per le successive attività ispettive e per l'acquisizione di tutte le ulteriori notizie ed atti.

Sarà quindi richiesto di dare evidenza circa:

- **tutto il software** presente in azienda ovvero installato negli elaboratori, memorizzato su eventuali supporti di riserva ai sensi dell'art. 64 ter della L. 633/1941, conservato su supporti originali;
- **documentazione** idonea a comprovare il legittimo possesso e/o utilizzo dei programmi ovvero contratti, accordi con produttore o distributore, documentazione originale del prodotto (n. licenza, chiave di accesso);
- **fatture di acquisto, ricevute fiscali o scontrini di cassa** comprovanti la regolarità dell'acquisto e del possesso.

Il personale della Guardia di Finanza chiederà quindi di avere accesso fisico e logico (passwords di accesso) alle dotazioni informatiche (PC, supporti di memorizzazione esterni) presenti e in uso presso la sede e completerà una rilevazione tecnica del contenuto di questi supporti per identificare e rilevare puntualmente i programmi installati e i file multimediali eventualmente presenti.

La verifica verrà poi estesa al materiale non installato e sui supporti presenti nel luogo delle verifiche ispettive.

A conclusione di questa fase verrà redatta una lista dei prodotti informatici presenti, che verranno quindi riconciliati con la documentazione amministrativa e fiscale che l'azienda avrà nel frattempo prodotto (es. fatture, documenti relativi alle licenze).

### Accertamento

Nel caso in cui la documentazione esibita dovesse comprovare solo in parte il legittimo possesso e/o utilizzo del software a disposizione o in uso, configurandosi le fattispecie penalmente rilevanti previste e punite dagli artt. 171 e 171 bis della L. 633/1941, il personale della Guardia di Finanza provvederà ad attuare successive operazioni di perquisizione e di sequestro al fine di acquisire ogni possibile evidenza circa illeciti e reati.

Completata quest'ultima fase verranno redatti opportuni verbali che costituiranno le notifiche circa gli eventuali illeciti.

### Contestazione e notifica

Come abbiamo già visto, oltre a integrare violazioni di natura penale, l'illecito relativo alla violazione del diritto d'autore comporta anche la violazione di natura amministrativa prevista all'art. 174 bis della L. 633/1941.

Gli agenti della Guardia di Finanza dovranno quindi procedere alla contestazione e notifica di una sanzione pecuniaria[17], il cui pagamento avrà effetto liberatorio per quanto riguarda il solo illecito amministrativo, mentre le violazioni riscontrate daranno seguito a successivi procedimenti di natura penale e quindi civile per la rivalsa dei diritti dei proprietari delle opere.

**17** La sanzione è pari al doppio del prezzo di mercato dell'opera o del supporto oggetto della violazione, in misura comunque non inferiore a euro 103 ovvero, se il prezzo non è rilevabile o determinabile, con una sanzione minima di euro 103 e massima di euro 1.032, applicabile nella misura stabilita per ogni violazione e per ogni esemplare abusivamente duplicato o riprodotto.

**Tabella 2** - Dettaglio delle sanzioni previste per la violazione della Legge sul Diritto d'autore

| Sanzioni | |
|---|---|
| CIVILI | Sequestro delle copie illecite sia su supporti che su dispositivi informatici, nonché degli eventuali proventi dovuti al legittimo autore dell'opera<br><br>Art. 161 L. 633/1941<br><br>1. Agli effetti dell'esercizio delle azioni previste negli articoli precedenti, nonché della salvaguardia delle prove relative alla contraffazione, possono essere ordinati all'Autorità giudiziaria la descrizione, l'accertamento, la perizia od il sequestro di ciò che si ritenga costituire violazione del diritto di utilizzazione; può inoltre farsi ricorso ai procedimenti d'istruzione preventiva. |
| | Emissione di ordine di inibitoria della violazione<br><br>Art. 163 L. 633/1941<br><br>1. Il titolare di un diritto di utilizzazione economica può chiedere che sia disposta l'inibitoria di qualsiasi attività che costituisca violazione del diritto stesso, secondo le norme del codice di procedura civile concernenti i procedimenti cautelari.<br><br>2. Pronunciando l'inibitoria, il giudice può fissare una somma dovuta per ogni violazione e inosservanza successivamente constatata o per ogni ritardo nell'esecuzione del provvedimento. |
| | Distruzione o rimozione degli oggetti e dei dispositivi da cui risulti la violazione<br><br>Art. 159 L. 633/1941<br><br>1. La rimozione o la distruzione prevista nell'art. 158 non può avere per oggetto che gli esemplari o copie illecitamente riprodotte o diffuse, nonché gli apparecchi impiegati per la riproduzione o diffusione che non sono prevalentemente adoperati per diversa riproduzione o diffusione.<br><br>2. Se gli esemplari, le copie e gli apparecchi di cui al comma 1 sono suscettibili, previa adeguata modifica, di una utilizzazione legittima da parte dell'autore della violazione, può essere disposto dal giudice il loro ritiro temporaneo dal commercio con possibilità di un loro reinserimento a seguito degli adeguamenti imposti a garanzia del rispetto del diritto.<br><br>3. Se una parte dell'esemplare, della copia o dell'apparecchio di cui al comma 1 può essere impiegata per una diversa riproduzione o diffusione, l'interessato può chiedere, a sue spese, la separazione di questa parte nel proprio interesse.<br><br>4. Il danneggiato può sempre chiedere che gli esemplari, le copie e gli apparecchi soggetti alla distruzione gli siano aggiudicati per un determinato prezzo in conto del risarcimento dovutogli.<br><br>5. I provvedimenti della distruzione e della aggiudicazione non colpiscono gli esemplari o le copie contraffatte acquistati in buona fede per uso personale.<br><br>6. L'applicazione delle misure di cui al presente articolo deve essere proporzionata alla gravità della violazione e tenere conto degli interessi dei terzi. |

Segue

| Sanzioni | |
|---|---|
| CIVILI | Avvio delle pratiche di risarcimento del danno<br><br>Art. 158 L. 633/1941<br><br>1. Chi venga leso nell'esercizio di un diritto di utilizzazione economica a lui spettante può agire in giudizio per ottenere, oltre al risarcimento del danno che, a spese dell'autore della violazione, sia distrutto o rimosso lo stato di fatto da cui risulta la violazione.<br><br>2. Il risarcimento dovuto al danneggiato è liquidato secondo le disposizioni degli artt. 1223, 1226 e 1227 del codice civile. Il lucro cessante è valutato dal giudice ai sensi dell'art. 2056 comma 2 del codice civile, anche tenuto conto degli utili realizzati in violazione del diritto.<br>Il giudice può altresì liquidare il danno in via forfettaria sulla base quanto meno dell'importo dei diritti che avrebbero dovuto essere riconosciuti, qualora l'autore della violazione avesse chiesto al titolare l'autorizzazione per l'utilizzazione del diritto.<br><br>3. Sono altresì dovuti i danni non patrimoniali ai sensi dell'art. 2059 del codice civile.<br><br>Pubblicazione accertamenti su quotidiani nazionali |
| PENALI | Reclusione da 3 a 6 anni |
| | Multa da 2.000 a 15.000 euro |

# 6. RIEPILOGO

I programmi software vengono considerati opere d'ingegno e come tali sono giuridicamente protetti dalla legge sul diritto d'autore; la legge vieta:

- la duplicazione dei programmi a scopo di profitto;
- l'importazione, la distribuzione, la detenzione, la vendita e il noleggio di copie illecite a scopo commerciale o imprenditoriale;
- la rimozione o l'elusione dei dispositivi di protezione appositamente apposti.

I programmi software vengono **contraffatti e distribuiti** o, più semplicemente, **illegalmente copiati e installati** per il loro utilizzo in a**mbito personale o professionale**.

In particolare, la detenzione e l'utilizzo di copie non originali costituiscono una **condotta illecita che rientra nella sanzione penale**, se relative all'uso commerciale, imprenditoriale o per scopo di profitto.

L'installazione di questo materiale su dispositivi informatici aziendali rende direttamente **responsabile** l'impresa e i suoi legali rappresentanti.

Controlli e verifiche ispettive vengono regolarmente eseguiti presso aziende e imprese.

Violazioni a queste norme di legge comportano **sempre una sanzione amministrativa e, nel caso di rilevanza penale, la denuncia all'autorità giudiziaria, la multa e sanzioni ausiliarie**, quali il sequestro dei dispositivi informatici contenenti i programmi contraffatti e la pubblicazione dei rilievi a mezzo stampa su un quotidiano nazionale.

L'azienda, tramite la propria organizzazione del lavoro, dovrebbe assicurarsi che:

- non venga installato software su computer o prodotti telematici di proprietà dell'impresa né vengano fatte copie del software licenziato all'impresa stessa;
- il materiale digitale protetto dal diritto d'autore sia gestito con apposite procure ed azioni di controllo sotto la supervisione di un responsabile aziendale dedicato;
- tutto il materiale documentale relativo all'acquisto, alle licenze nonché all'assegnazione dei prodotti software in azienda sia custodito diligentemente e sia disponibile per tutta la durata di vita del prodotto e non sia oggetto di eventuali copie da parte dei dipendenti o di terzi;
- il personale riceva apposite istruzioni per la gestione del rischio.

## GLOSSARIO

### CHIAVE DI ACCESSO
Accredito per l'accesso telematico a un determinato servizio informatico, consistente generalmente in un nominativo di riconoscimento (ID User – Identificativo utente) e di una parola chiave (password) assegnati a singoli utenti per definirne il profilo e l'autorità di accesso ai dati e ai programmi erogati dal servizio.

### CLIENT
Dispositivo informatico che accede ai servizi o alle risorse di un'altra componente, detta server. Può essere tipicamente un computer collegato a un computer centrale (server) tramite una rete informatica (locale o geografica) e al quale richiede uno o più servizi, utilizzando uno o più protocolli di rete, oppure un componente (client software) di un sistema di posta elettronica. Sempre più soluzioni software sono infatti divise in una parte client (residente e in esecuzione sul pc client) ed una parte server (residente e in esecuzione sul server).

### CODICE DI LICENZA
Sequenza alfanumerica univocamente assegnata a ciascuna copia fisica o digitale di un prodotto software per la sua successiva identificazione e distribuzione. Il codice licenza è normalmente riportato all'interno del documento contrattuale di licenza, nonché stampato sui supporti con cui il prodotto è commercializzato.

### CODICE DISCIPLINARE
Insieme delle norme e istruzioni, introdotte a partire dallo Statuto dei Lavoratori, per stabilire le corrette normative aziendali interne, che i dipendenti sono chiamati a rispettare in virtù degli obblighi di diligenza, obbedienza e fedeltà (artt. 2104, 2105 C.C.).

### CODICE APPLICATIVI/INFORMATICI
Linguaggio in codice informatico con cui sono scritti i programmi eseguiti dagli elaboratori elettronici o dalle unità di elaborazione di dispositivi (telefoni palmari, console videogiochi).

### CONTRASSEGNO SIAE

Speciale contrassegno, comunemente denominato bollino SIAE, che dovrebbe essere apposto su ogni supporto contenente opere protette dal diritto d'autore. Dal punto di vista tecnico, il bollino è difficilmente riproducibile (ologramma con elementi non rilevabili ad occhio nudo), o rimovibile e riporta il titolo dell'opera, il nome del produttore e la numerazione progressiva relativa a quell'opera.

### DIRITTO D'AUTORE

Posizione giuridica soggettiva di un autore di un'opera dell'ingegno a cui i diversi ordinamenti nazionali e varie convenzioni internazionali (quale la Convenzione di Berna) riconoscono la facoltà esclusiva di diffusione e sfruttamento dell'opera prodotta. In Italia il diritto è disciplinato prevalentemente dalla L. 633/1941 e successive modificazioni e dal Titolo IX del Codice Civile.

### DOWNLOAD / UPLOAD

Operazione con la quale si trasferiscono dati (file, programmi, codici) fra due dispositivi informatici connessi da una rete telematica. Per eseguire queste funzione vengono attivati su entrambe le unità particolari programmi di trasmissione (es. Napster) e, attraverso protocolli (es. FTP) predefiniti, viene automaticamente gestito il trasferimento dei dati da una macchina all'altra. A seconda che il dato sia inviato o ricevuto, l'operazione viene riferita come upload o download.

### FILE SHARING

Condivisione di file all'interno di una rete telematica. Può essere eseguita con una architettura logica di tipo client-server (cliente-servente) in cui, con operazioni di tipo upload/download vengono distribuiti o prelevati dati fra unità, oppure di tipo peer-to-peer (pari a pari o P2P) in cui ogni utente mette a disposizione degli altri utenti della medesima rete dati e risorse che possono essere fruite e prelevate liberamente (File sharing).
In Internet le più famose reti di peer-to-peer sono: Gnutella, OpenNap, Bittorrent, eDonkey, Kademlia. Queste reti possono permettere di individuare più copie dello stesso file disponibili nella rete, di eseguire l'acquisizione da più fonti contemporaneamente, di ricercare autonomamente un file fra le unità presenti nella rete.

FIREWALL
Server (dispositivo informatico o computer) interconnesso con una rete privata (rete aziendale) e una rete pubblica (Internet) programmato per verificare e filtrare gli accessi telematici fra queste due reti, consentendo il solo transito di dati e operazioni autorizzate in base alla programmazione del server. Costituisce l'infrastruttura primaria per la sicurezza di una rete aziendale e dei computer ad essa collegati.

FREEWARE
Software che viene distribuito in modo totalmente gratuito. È sottoposto esplicitamente a una licenza che ne permette la redistribuzione gratuita e viene concesso in uso senza alcun corrispettivo. È liberamente duplicabile e distribuibile, con pochissime eccezioni. Da non confondersi con i programmi di tipo shareware che, nonostante siano distribuiti in maniera simile a quelli freeware, richiedono un pagamento al termine di un periodo di prova o per attivarne tutte le funzionalità disponibili.

HIGH BAND
Rete telematica o connessione con caratteristiche di elevata capacità di trasporto dei dati e di velocità di connessione. Ordinariamente si tratta di connessioni di tipo ADSL per utenze domestiche e T1 per utenze aziendali.

INFORMATICA DI REPARTO O D'UFFICIO
Dispositivi informatici che vengono usati presso l'azienda e che non sono formalmente assegnati a singoli dipendenti/utenti. Benché l'accesso logico alle applicazioni di queste macchine avvenga sempre attraverso l'identificazione dell'utente (vedi chiave di accesso), le risorse dell'unità, quali ad esempio la memoria su supporti hdd (dischi), possono essere utilizzate indistintamente da tutti coloro che hanno accesso alla macchina.

LICENZA D'USO
Insieme delle condizioni contrattuali che specificano le modalità con cui l'utente può usare il prodotto, garantendo diritti e definendo obblighi.
La licenza è imposta da chi detiene il copyright sul prodotto software.
L'accettazione della licenza da parte dell'utilizzatore può avvenire in diversi modi: con l'uso stesso del programma, durante la fase di installazione del software, prima di venire in possesso del programma, prima di aprire le custodie dei supporti di massa dove sono registrati i programmi acquistati.

MALWARE
Codice o programma software creato allo scopo di causare danni al sistema informatico in cui viene eseguito. Deriva dalla combinazione dei termini malicius e software.

MODEM
Dispositivo elettronico che rende possibile la comunicazione fra sistemi informatici o singoli computer, utilizzando un canale di comunicazione composto tipicamente da una rete telefonica.

P2P
Vedi file sharing.

PIATTAFORMA INFORMATICA
Termine generico per indicare un dispositivo o un sistema di elaborazione dati. Può essere costituita da un computer portatile interconnesso ad una rete aziendale, denominato sistema client, e da un insieme di dispositivi informatici operanti presso una sede e denominati server, il cui scopo è quello di erogare servizi e dati per mezzo di una rete telematica e tramite l'uso di specifiche applicazioni informatiche.

PIRATERIA SOFTWARE/SOFTWARE PIRACY
Il termine indica la violazione del diritto di utilizzo e distribuzione di un programma per elaboratore (software) sulla base delle condizioni rilasciate originariamente dall'autore o dal detentore dei diritti economici del prodotto. Tali violazioni possono essere perpetrate duplicando, utilizzando, modificando o distribuendo (in copia fisica o tramite reti telematiche) illecitamente il programma software.

PRODOTTI PROGRAMMA
L'insieme di programmi per elaboratore che costituiscono di norma un prodotto commercializzato.

PROPRIETÀ INTELLETTUALE
Sistema di tutela giuridica dei beni immateriali derivati dall'attività creativa/inventiva umana come ad esempio le opere artistiche e letterarie, le invenzioni industriali e i modelli di utilità, il design, i marchi a cui fanno capo le tre grandi aree del diritto d'autore, del diritto dei brevetti e del diritto dei marchi.

PROTOCOLLI DI COMUNICAZIONE
Insieme di regole formalmente descritte, definite al fine di favorire la comunicazione tra uno o più sistemi presenti su una rete telematica.
L'aderenza ai protocolli garantisce che due software in esecuzione su macchine anche diverse fra loro (computer, telefono, stampante) possano interagire correttamente anche se sono realizzate indipendentemente una dall'altra.

RESPONSABILITÀ GIURIDICA
Consiste nell'obbligo o nelle obbligazioni che derivano dall'esecuzione di atti da parte di singoli, società, enti o pubbliche amministrazioni.
La responsabilità giuridica può essere civile, penale amministrativa oltreché contabile e disciplinare.

SCOPO DI LUCRO
Dal punto di vista giuridico-economico, si intende un introito per vendita o guadagno monetario che derivi ad un dato soggetto.

SCOPO DI PROFITTO
Dal punto di vista giuridico-economico, si intende ogni vantaggio economico che derivi ad un dato soggetto, in forza di un rapporto giuridico o di un fatto naturale o di un mero comportamento umano.

SERVER
È un elaboratore che eroga servizi informatici ad altre componenti identificati come client, attraverso una rete dati. A seconda del contesto, il termine server può indicare un computer utilizzato per fornire servizi ad altri computer, un computer appartenente ad una particolare fascia di mercato dedicata all'uso come server caratterizzata da alta affidabilità e prestazioni, un programma software in esecuzione che fornisce servizi ad altri processi del medesimo ambiente applicativo.

SHAREWARE
Software che viene distribuito in modo simile al freeware, ma richiede un pagamento al termine di un periodo di prova prestabilito o per attivarne alcune funzionalità specifiche non di base.

### SISTEMI ANTICOPIA

Sono sistemi tecnologici mediante i quali i titolari di diritto d'autore rendono protette, identificabili e tracciabili le loro opere digitali. I file così prodotti portano con sé le diciture di copyright. L'accesso ai contenuti da parte degli utenti finali avviene secondo procedure di autenticazione che permettono fra l'altro di usare e distribuire i file richiesti unicamente nelle modalità previste dalla licenza sottoscritta dall'utente stesso.
Questi prodotti sono anche chiamati "filigrana digitale", in quanto le informazioni nascoste che vengono aggiunte ai file hanno lo scopo di proteggere il prodotto analogamente alla filigrana delle banconote.

### SISTEMI DI PROTEZIONE

Tutti i sistemi fisici e logici atti a proteggere un prodotto software dalle possibili violazioni informatiche.

### TRY & BUY

Modalità di distribuzione di programmi software che prevede un periodo limitato e predefinito in cui l'utente gratuitamente potrà usare il prodotto nel proprio ambiente operativo, dopo di ché potrà acquistarne regolare licenza d'uso per proseguirne l'utilizzo.

### WIFI

Rete relativamente economica e di veloce attivazione che permette di realizzare sistemi flessibili per la trasmissione di dati usando frequenze radio, estendendo o collegando reti fisiche esistenti ovvero creandone di nuove. Wi-Fi, abbreviazione di Wireless Fidelity, è inoltre un termine che indica i dispositivi che possono collegarsi a reti locali senza fili.

**Bibliografia consigliata**

S. Aliprandi, *Copyleft e opencontent,* Primaora, 2005
R. Borruso, *Computer e diritto,* Giuffrè, 1988
R. Borruso, *La tutela giuridica del software,* Giuffrè, 1998
G. Ceccaci, *Computer crimes,* FAG, 1994
G. De Sanctis, *La tutela giuridica del software tra brevetto e diritto d'autore, Giuffrè, 2000*
V. Franceschelli, E. Tosi, *Il codice della proprietà intellettuale e industriale,* CELT, 2009
A. Gaudenzi, *Il nuovo diritto d'autore,* Maggioli Editore, 2009
A. Patron, *Il nuovo diritto d'autore,* Ed. Giuridiche Simone, 2001
G. Pica, *Il diritto penale delle tecnologie informatiche,* UTET, 1999
C. Prodi, A. Calice, *Responsabilità penali e Internet,* IlSole24ore, 2001
G. Ziccardi, *Il diritto d'autore nell'era digitale,* IlSole24ore, 2001

**Siti utili**

www.assolombarda.it
www.BSA.org
www.guardiadifinanza.it

ISBN 9788890484049

ASSOLOMBARDA

via Pantano, 9
20122 Milano
mitoz@assolombarda.it
www.assolombarda.it